楕円曲線入門

J. W. S. キャッセルズ 著
徳永浩雄訳

岩 波 書 店

LECTURES ON ELLIPTIC CURVES

by J. W. S. Cassels

First published 1991 by the Press Syndicate of
the University of Cambridge, Cambridge.

This Japanese edition published 1996
by Iwanami Shoten, Publishers, Tokyo
by arrangement with
the Syndicate of the Press of the University of Cambridge, Cambridge.

目　　次

序 *1*

1　種数 0 の曲線：序論 *3*

2　p–進　数 *7*

3　2 次曲線に関する局所–大域原理 *15*

4　数の幾何学 *21*

5　局所–大域原理（証明の完結） *25*

6　3 次曲線 *29*

7　非特異 3 次曲線と群構造 *33*

8　楕円曲線とその標準形 *39*

9　退化した曲線の群構造 *47*

10　還　　元 *51*

11　p–進体上の楕円曲線 *57*

12　有限位数の元 *63*

13　有限生成定理（証明の方針） *69*

14　2–同種写像 *75*

15　弱有限生成定理 *85*

16　補足：終結式 *95*

17　高さと有限基底定理の証明 · · · · · · · · · · · 99

18　種数が 1 の曲線に関する局所–大域原理 · · · 107

19　ガロアコホモロジーの初歩 · · · · · · · · · · · 113

20　ヤコビ多様体の構成 · · · · · · · · · · · · · · 117

21　抽象論からの準備 · · · · · · · · · · · · · · · 125

22　主等質空間とガロアコホモロジー · · · · · · · 133

23　Tate–Shafarevich 群 · · · · · · · · · · · · · · 139

24　自己準同型環 · · · · · · · · · · · · · · · · · 145

25　有限体上定義された楕円曲線の有理点 · · · · 151

26　楕円曲線を用いた因数分解 · · · · · · · · · · 157

付録A　公 式 集 · · · · · · · · · · · · · · · · · 165

付録B　参 考 書 · · · · · · · · · · · · · · · · · 171

訳者あとがき · · · · · · · · · · · · · · · · · · · 173

索　　引 · 175

序

Diophantos 方程式――すなわち，代数方程式の整数解もしくは有理数解を求めること――は古来，我々を魅了してきた: 実際，紀元前1600年から紀元前1900年の間のバビロニアの文献には，ピタゴラスの方程式

$$X^2+Y^2=Z^2$$

の15種類の解が書かれている．Diophantos 自身は3世紀にアレキサンドリアに住んでいた人で，現在も彼の業績のいくつかには触れることができる．Diophantos の仕事は Hypatia により受け継がれた．Hypatia は古代の女性数学者で今日まで名前の残っている唯一の数学者である．もう一人，現在においても影響の大きい数学者は Fermat (1601–1665) である．現代的な視点からみた歴史に関しては，A. Weil の著作 *Number theory: an approach through history from Hammurabi to Legendre*, Birkhäuser, 1983 (邦訳) 足立恒雄・三宅克哉(訳)，数論――歴史からのアプローチ, 日本評論社, 1987 を参照するとよい．[Hypatia については Gibbon の *Decline and Fall* 参照.]

本書では，Diophantos 方程式の有理数解に重点をおいている．整数解についてはより深い考察が必要であり，本書では触れない．

さて，Diophantos 方程式のいろいろな側面を記述する言葉として代数幾何学の用語を用いるのが適当であるのは明らかである: とはいえ，複素数体上で展開する古典的な代数幾何学ではなく，基礎体が有理数体 $\boldsymbol{Q}$ などの上のものである．これはしばしば “Diophantos 幾何学” とよばれる．古典的な代数幾何学の結果や議論のうち，Diophantos 幾何学にそのまま適用できるものもあれば，結論に制限が加わるもの，また，さらに仮定(古典的な場合は自動的にみたされているような)をつけ加えなければならないものなどもある．

Diophantos 方程式は代数多様体上の点の存在に関する問題としてとらえられる．本書では曲線についてのみ考える．幾何学者は種数という非負整数

を用いて曲線を分類している．種数が 0 のときの Diophantos 理論はよく知られている．種数が 1 の曲線については非常に豊富な内容をもつ理論が確立されており，また最近の集中的な研究により解明されつつある予想などの根源にもなっている．種数が 1 より大きい曲線の Diophantos 理論はまだ(Faltings の定理はあるが)始まったばかりである．

本書の主な目的は，種数が 1 の曲線の Diophantos 理論を紹介することである．その状況を明確にするため，本書ではまず種数が 0 のときの結果を解説することから始める．そこでは局所–大域原理(Hasse 原理)がすべてを支配する．これは $\boldsymbol{Q}$ 上の状況を局所的な完備化，$\boldsymbol{Q}_p$ の上のものに結びつけるものである．種数が 1 のときの主題は，局所的(p–進的)なふるまいが有理数体上のふるまいを決めるというところまでである．この内容は代数体までスムーズに一般化できるが，本書では新しい概念は単純な状況で考えるのがもっとも理解しやすいという信念にもとづき，有理数体上でのみ考える．

最後の 3 章では目的を少し変える．3 つのうち 2 つの章では，(種数 1 の) "関数体上の Riemann 予想" を頂点とする，有限体上のより洗練された理論を紹介する．最後の章では，これらの理論が大きな整数を因数分解するための現代のテクノロジーにどのように使われているかを解説する．

本書を読むための予備知識について

本書では必要となる予備知識は最小限におさえてある．種数が 0 や 1 の曲線という言葉はすでに使ったが，実際に扱うのは 2 次曲線や平面 3 次曲線といった具体的な曲線が中心である．p–進数については最初から解説してある．また，代数的整数論からの知識は，読者が 1 つの主張を認めることにすれば必要ではない．しかしながら，本文の一部で示しているように，多くの応用を考える上では代数的整数論は不可欠である．ガロア理論の初歩については仮定する：実際，その応用は興味深い．

1

種数 0 の曲線：序論

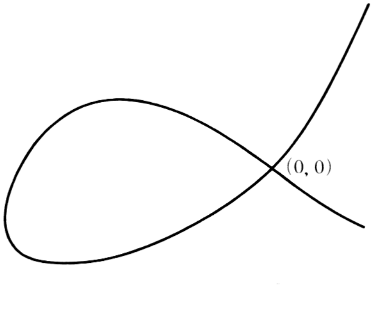
まず，最初に言葉をいくつか定義しよう．点の座標が有理数であるとき，その点は**有理的**である，または**$\boldsymbol{Q}$ 上定義**されているという．また，曲線が $\boldsymbol{Q}$ 係数の代数方程式の零点集合で与えられているとき，その曲線は**$\boldsymbol{Q}$ 上定義**されているという．[残念ながら，有理曲線という言葉はすでに幾何学者たちにより種数 0 の曲線の意味で使われているので，ここでは使えない.] 一般的にいって，"$\boldsymbol{Q}$ 上で考える" というときは，でてくる代数的なもの(方程式など)がすべて $\boldsymbol{Q}$ 係数であることを意味する．

$\boldsymbol{Q}$ 上で考えるときには，初等幾何学的手法がそのまま有効なときがある．例えば，3 次曲線

$$\mathcal{C}:\ \ X^2-Y^2=(X-2Y)(X^2+Y^2)$$

を考えてみよう(この曲線は原点で 2 重点をもっている)．

原点を通る直線は $\mathcal{C}$ ともう 1 点で交わるが，これが $\mathcal{C}$ 上の点に関する 1 つ



の記述を与える．正確には，s という与えられた数に対し直線 $X=sY$ を考えれば，この直線は y 座標が

$$Y^2(s^2-1)=Y^3(s-2)(s^2+1)$$

をみたす点で $\mathcal{C}$ と交わる．つまり，$(0,0)$ と点 (x,y)，ただし，

$$x=\frac{s(s^2-1)}{(s-2)(s^2+1)},\quad y=\frac{s^2-1}{(s-2)(s^2+1)}$$

で交わる．

逆に，$\mathcal{C}$ 上の点 (x,y) が与えられたとき，$s=x/y$ とおけば，(x,y) は s を用いて上記のように表される．つまり，$\mathcal{C}$ は直線に**双有理同値**である．この例の場合，その双有理同値写像は $\boldsymbol{Q}$ 上定義されている．[つまり，双有理同値が $\boldsymbol{Q}$ 係数の有理関数で与えられている．ここで，“有理”という言葉がもう 1 つの別の意味で使われていることに注意 !]

一般に双有理写像が 2 つの曲線間に与えられているとき，一方から他方へ有理点の間に有限個の例外を除いて写像 1 対 1 対応がある．例外点としては，例えば上記の例では $s=2$ に対応する点 (x,y) は存在しない．また，$s=\pm1$ は共に $(x,y)=(0,0)$ にうつされる．さらに，$\mathcal{C}$ の定義式の左辺 X^2-Y^2 を X^2-2Y^2 にとりかえると $(x,y)=(0,0)$ は s の有理数値に対応しない．とはいえ，2 つの曲線が $\boldsymbol{Q}$ 上双有理同値であれば，上記のような例外点が有限個であることを証明するのは難しくないのである．つまり，曲線の有理点を調べるには，$\boldsymbol{Q}$ 上の双有理同値を除いて調べればよいことがわかる．

複素数体 $\boldsymbol{C}$ 上で成立する古典的な定理に，“種数 0 の曲線はすべて，直線に双有理同値である”がある．この定理は $\boldsymbol{Q}$ 上では成立しないが，そのかわりに次の事実が成立する．

事実　$\boldsymbol{Q}$ 上定義された種数 0 の曲線は，直線または 2 次曲線に双有理同値である．　□

この事実により，種数 0 の曲線の Diophantos 理論は，2 次曲線のそれに帰着される．

定理 1　有理点をもつ 2 次曲線は $\boldsymbol{Q}$ 上双有理同値である．逆に，$\boldsymbol{Q}$ 上定義された 2 次曲線が直線に $\boldsymbol{Q}$ 上双有理同値ならば，その 2 次曲線は有理点

をもつ．

［証明］　後半は明らか．したがって，前半のみを証明する．2 次曲線上に有理点があるとする．座標をとりかえて，その点が原点であると仮定してよい．すると，この 2 次曲線の方程式は，

$$F_1(X,Y)+F_2(X,Y)=0,$$

F_j は X,Y に関する次数 j の同次式，と書ける．この状況の下で双有理同値を得るには，前の 3 次曲線同様

$$X=sY$$

とおいて得られる．■

こうして，種数 0 の曲線の Diophantos 理論は，$\boldsymbol{Q}$ 上定義された 2 次曲線がいつ有理点をもつかということに帰着される．ところで，有理点をもたない 2 次曲線の例を与えることは簡単である．それを示すため，ここからは，同次座標を用いることにしよう．2 次曲線

$$X^2+Y^2+Z^2=0$$

上には有理点はない．なぜなら，この 2 次曲線上には明らかに実数点がないからである．さらに，2 次曲線

$$X^2+Y^2-3Z^2=0 \tag{$*$}$$

上には有理点はない．実際，点 (x,y,z) がこの 2 次曲線の有理点であったとしよう．同次性を用いて x,y,z は互いに素な整数としてよい．さて，$(*)$ から $x^2+y^2\equiv 0\ (3)$，したがって，$x\equiv y\equiv 0\ (3)$ である．ゆえに $(*)$ から $z\equiv 0\ (3)$ が得られるが，これは，x,y,z がすべて 3 で割り切れることを示し，仮定に反する．

ところで，今の最後の議論を異なった方法で表現することが便利であるし，ひいては不可欠でもある．つまり，p–進数体 $\boldsymbol{Q}_p$（p は素数，上記の例では $p=3$）の導入である．すなわち，最後の例は，$(*)$ が "$\boldsymbol{Q}_3$ 上で解をもたない" ことを証明したことにほかならないのである．

2

p − 進　数

実数体や複素数体の普通の絶対値の性質のうち，もっともよく知られたものは次の3つであろう．

（i） $|r| \geqq 0$，等式は $r=0$ のときのみ成立．

（ii） $|rs|=|r||s|$．

（iii） $|r+s| \leqq |r|+|s|$．

体 k 上の実数値関数 $|\ \ |$ で，上記の(i)，(ii)，(iii)の性質をみたすものは**付値**(valuation)とよばれる．$(-1)^2=1$ であるから，(i)–(iii)より $|-1|=1$ であり，またすべての r に対して $|-r|=r$ を得る．

有理数体 $\boldsymbol{Q}$ は絶対値以外の付値をもつ．素数 p を1つ固定する．0でない任意の有理数 r は次のような形に書ける．

$$r = p^{\rho}u/v, \qquad \rho \in \boldsymbol{Z},\ u, v \in \boldsymbol{Z},\ p \nmid u,\ p \nmid v.$$

付値 $|r|_p$ を0以外の元に対しては

$$|r|_p = p^{-\rho},$$

0に対しては

$$|0|_p = 0$$

で定義する．この定義で $|\ \ |_p$ が条件の(i)，(ii)をみたすのは明らかであろう．(iii)を調べるために s を

$$s = p^{\sigma}m/n, \qquad m, n \in \boldsymbol{Z},\ p \nmid m,\ p \nmid n$$

とおけば，

$$|s|_p = p^{-\sigma}$$

である．一般性を失うことなく

$$\sigma \geqq \rho, \quad \text{すなわち}, \quad |s|_p \leqq |r|_p$$

としてよい．すると

$$r+s = p^{\rho}(un+p^{\sigma-\rho}mv)/vn$$

を得る．ここで，$p \nmid vn$ であり，分子 $un+p^{\sigma-\rho}mv$ は p を約数にもちうる整数である．したがって，

$$|r+s|_p \leqq p^{-\rho}$$

が得られ，これから

(iii*)　$|r+s|_p \leqq \max\{|r|_p, |s|_p\}$

を得る．(iii*)から(iii)が得られるのは明らかであるから，$|\quad|_p$ は付値となることがわかる．この付値は p–**進付値**とよばれる．**三角不等式**(iii)は $|r-s|$ が距離を与えることを示しているので，不等式(iii*)は**超距離不等式**(ultrametric inequality)ともよばれる．超距離不等式をみたす付値は**非アルキメデス的付値**とよばれる．

普通の絶対値で親しんでいる用語はそのまま p–進付値のそれへおきかえることができる．例えば，数列 $\{a_n\}$, $n=1,2,\cdots$ が**基本列**であるとは，次の条件をみたすことをいう：任意の $\varepsilon>0$ に対して，$m,n \geqq n_0(\varepsilon)$ ならば，$|a_m-a_n|_p<\varepsilon$ が成り立つような $n_0(\varepsilon)$ が存在する．

数列 $\{a_n\}$ が b に**収束**するとは，任意の $\varepsilon>0$ に対して $n \geqq n_0(\varepsilon)$ ならば，$|a_n-b|_p<\varepsilon$ が成り立つような $n_0(\varepsilon)$ が存在することをいう．

例えば，

$$p=5$$

とし，数列

$$\{a_n\}: \quad 3, \quad 33, \quad 333, \quad 3333, \quad \cdots$$

を考える．すると

$$a_m \equiv a_n \quad (5^n) \qquad (m \geqq n).$$

すなわち，

$$|a_m - a_n|_5 \leqq 5^{-n} \qquad (m \geqq n).$$

ゆえに $\{a_n\}$ は基本列である．実際，

$$3a_n = 99\cdots 99 \equiv -1 \quad (5^n),$$

つまり，

$$|3a_n+1|_5 \leqq 5^{-n}.$$

したがって，5–進的にはこの数列は

$$a_n \to -1/3$$

に収束する．この例でわかるように，p–進付値に関する難しさは心理的なものである：　p–進的に小さいとはそれが p の高いベキで割り切れるということである．p–進基本列がすべて収束列というわけではない．例えば，ここでまた $p=5$ とし，以下，数列 $a_n \in \boldsymbol{Z}$ を

$$a_n^2+1 \equiv 0 \quad (5^n)$$

かつ

$$a_{n+1} \equiv a_n \quad (5^n)$$

をみたすように構成する．まず $a_1=2$ とおく．いま a_n まですでに定まったとして，$a_{n+1}=a_n+b5^n$ とおく．ここで b が問題となる数字である．まず b は

$$(a_n+b5^n)^2+1 \equiv 0 \quad (5^{n+1})$$

をみたさねばならない．ここで

$$c = (a_n^2+1)/5^n$$

とおけば仮定から c は整数であり，b のみたすべき式は

$$2a_nb+c \equiv 0 \quad (5) \tag{$*$}$$

となる．明らかに $5 \nmid a_n$ であるから，$(*)$を b について解いてこれを決めることができる．すなわち，a_{n+1} を得る．

こうして得られた数列 $\{a_n\}$ は

$$|a_m-a_n|_5 \leqq 5^{-n} \qquad (m \geqq n)$$

をみたすから 5–進基本列である．

いま a_n が 5–進的に $\boldsymbol{Q}$ の元 e に収束するとしよう．すると

$$a_n^2+1 \to e^2+1.$$

一方，a_n の作り方から，

$$a_n^2+1 \to 0.$$

したがって，$e^2+1=0$ となるがこれは矛盾である．

実数が有理数体を絶対値に関して完備化して得られるように，有理数体を $|\ \ |_p$ で完備化すれば，**p-進体 $\boldsymbol{Q}_p$** が得られる．実際，$|\ \ |_p$ は非アルキメデス的付値なのでそのプロセスは簡単である．が，実数をどのようにして得るかということに慣れてない読者のために，この章の終りでどのようにして $\boldsymbol{Q}_p$ を得るかを簡単に述べよう．

体 K が付値 $|\ \ |$ に関して **"完備"** であるとは，すべての基本列が収束するときをいう．付値 $\|\ \ \|$ をもつ体 K が付値 $|\ \ |$ をもつ体 k の**完備化**であるとは，k から K への単射

$$\lambda:\ k \to K$$

で付値を保ち：

$$\|\lambda a\| = |a| \qquad (a \in k)$$

かつ，次の条件をみたすものが存在することをいう．

（i） K は $\|\ \ \|$ に関し完備，

（ii） K は λk の閉包である（すなわち K はそれほど大きくない）．

完備化は常に存在し，同型を除けば一意的である．したがって，k と λk，$|\ \ |$ と $\|\ \ \|$ を同一視し，k を K の部分体とみなすことにする．

さて，付値 $|\ \ |_p$ をもった p-進体 $\boldsymbol{Q}_p$ の構造を考えよう．

まず，

$$|b|_p < |a|_p \quad ならば \quad |a+b|_p = |a|_p$$

である．実際，(iii*) より，$|a+b|_p \leqq |a|_p$ であり，$a=(a+b)+(-b)$ であるから，もし $|a+b|_p<|a|_p$ なら矛盾である．この事実から，$\boldsymbol{Q}_p$ 上 $|\ \ |_p$ のとる値域は $\boldsymbol{Q}$ 上のそれと一致することがわかる．実際，$\alpha \in \boldsymbol{Q}_p$，$\alpha \neq 0$ をとれば，完備化の定義(ii)より，$|a-\alpha|_p<|\alpha|_p$ をみたす $a \in \boldsymbol{Q}$ が存在するので，$|\alpha|_p = |a|_p$ を得る．

$\boldsymbol{Q}_p$ の元 α で $|\alpha| \leqq 1$ をみたすものの集合は **p-進整数環**とよばれ，$\boldsymbol{Z}_p$ と表される．実際，$|\ \ |_p$ は非アルキメデス的であるから $\boldsymbol{Z}_p$ は環である：

$$|\alpha|_p,\ |\beta|_p \leqq 1 \quad \Rightarrow \quad |\alpha\beta|_p \leqq 1, \quad |\alpha+\beta|_p \leqq 1.$$

有理数 b は $b=u/v$，$u,v\in \boldsymbol{Z}$，$p\nmid v$ と書けるときに限り $\boldsymbol{Z}_p$ の元となる．

$\boldsymbol{Q}_p$ の元 ε で $|\varepsilon|=1$ をみたすものは p–進単数である．$\boldsymbol{Q}_p$ 上の $|\ \ |_p$ の値域に関し上で述べたことから，$\boldsymbol{Q}_p$ の 0 でない元 β は $\beta=p^n\varepsilon$（ただし，$n\in\boldsymbol{Z}$ で ε は単数）という形をしているとしてよい．単数は $\boldsymbol{Q}_p$ の元 ε で $\varepsilon\in\boldsymbol{Z}_p$，$\varepsilon^{-1}\in\boldsymbol{Z}_p$ をみたすものである．

すでに注意したように，解析の初等的な事実が $\boldsymbol{Q}_p$ で成立するが，それは以下に示すように簡単に証明される．

補題 1　$\boldsymbol{Q}_p$ において級数 $\sum\limits_0^\infty \beta_n$ が収束する必要十分条件は，$\beta_n\to 0$ $(n\to\infty)$ となることである．

［証明］　級数が収束するとは，もちろん部分和 $\sum\limits_0^N$ がある極限値に収束することを意味する．

級数が収束すれば $\beta_n\to 0$ となることは，普通の解析でも成り立つことである．逆を証明するには，超距離不等式(iii*)を複数の和に応用して簡単に得られる式

$$\begin{aligned}\left|\sum_0^N-\sum_0^M\right|_p &= \left|\sum_{M+1}^N \beta_n\right|_p\\ &\leqq \max_{M<n\leqq N}|\beta_n|_p\end{aligned}$$

に注意する．これから $\left\{\sum\limits_0^N\beta_n\right\}$ が基本列であることがわかり，$\boldsymbol{Q}_p$ の完備性からある極限値に収束することがわかる．∎

さてここで $\boldsymbol{Z}_p$ のはっきりした記述を与えよう．まず，

$$\mathcal{A}=\{0,1,\cdots,p-1\}$$

とおく．

補題 2　$\boldsymbol{Z}_p$ の元は次のようにして表される元全体と一致する：

$$\alpha=\sum_0^\infty a_np^n,$$

ただし

$$a_n\in\mathcal{A}\qquad(\text{すべての }n).$$

［証明］　前の補題からこの無限和は収束し，その収束値は $\boldsymbol{Z}_p$ の元である．

逆に $\boldsymbol{Z}_p$ の元 α が与えられたとする．$\boldsymbol{Q}$ の元 b で $|b-\alpha|_p<1$ をみたすものをとる．この b に対し，$|a_0-b|_p<1$ をみたす $\mathcal{A}$ の a_0 がただ1つ存在することは容易にわかる．この a_0 に対し，

$$\alpha=a_0+p\alpha_1 .$$

ただし，$|\alpha_1|\leqq 1$，すなわち，$\alpha_1\in\boldsymbol{Z}_p$ である．これを帰納的に続けていけば

$$\alpha=a_0+a_1p+\cdots+a_Np^N+\alpha_Np^{N+1}\qquad(\alpha_N\in\boldsymbol{Z}_p)$$

を得る．▮

次の最後の結果を得るには，$p=2$ のときと $p\neq 2$ のときを区別せねばならない．

補題 3 ($p\neq 2$)　α は $\boldsymbol{Q}_p$ の単数とする．$\alpha=\beta^2$ をみたす $\boldsymbol{Q}_p$ の元 β が存在するための必要十分条件は，$\boldsymbol{Q}_p$ の元 γ で

$$|\alpha-\gamma^2|_p<1$$

をみたすものが存在することである．

［証明］　必要性は明らかである．実は $p=5$, $\alpha=-1$ という特別な場合にすでに十分性を証明しているのであるが，一般の場合も同様である．つまり，$\beta_1=\gamma, \beta_2, \beta_3, \cdots$ を

$$|\beta_n^2-\alpha|\leqq p^{-n}$$

$$|\beta_{n+1}-\beta_n|\leqq p^{-n}$$

をみたすように帰納的に定めていけばよい．いま，β_n が得られたとして，$\beta_{n+1}=\beta_n+\delta$ とおけば

$$\beta_{n+1}^2=\beta_n^2+2\beta_n\delta+\delta^2$$

であるから，

$$\delta=(\alpha-\beta_n^2)/2\beta_n$$

とおけば条件をみたすように β_{n+1} が得られる．▮

この補題3は $p=2$ のときは成り立たない（$\alpha=5$, $\beta=1$ のときを考えよ）．$p=2$ では次の補題が成立する．

補題 4 ($p=2$)　α は $\boldsymbol{Q}_2$ の単数とする．$\alpha=\beta^2$ をみたす $\boldsymbol{Q}_2$ の元 β が存在するための必要十分条件は，

$$|\alpha-1|\leqq 2^{-3}$$

である．

［証明］　ここでもまた必要性は明らかである．十分性に関しては，前補題のように数列 $\beta_1=1, \beta_2, \beta_3, \cdots$ を構成して証明する．詳細は読者にまかせることにする．　■

$\boldsymbol{Q}_p$ の構成に関する概略を述べてこの章を終えよう．

$|\ \ |_p$ に関する基本列 $\{a_n\}$ ($\{a_n\}\in\boldsymbol{Q}$) の集合を $\mathfrak{F}$ で表す．$\mathfrak{F}$ は成分ごとのたし算，かけ算で環になる．

$$\{a_n\}+\{b_n\}=\{a_n+b_n\}:\ \{a_n\}\{b_n\}=\{a_nb_n\}.$$

数列 $\{a_n\}$ は $a_n\to 0$ (p–進的に) となるとき零列である．零列全体の集合を $\mathfrak{N}$ とすれば，これは明らかに $\mathfrak{F}$ のイデアルである．

$\{a_n\}$ を $\mathfrak{N}$ に含まれない $\mathfrak{F}$ の元とする．すると $n>N$ なるすべての n に対して，$|a_N-a_n|<|a_N|_p$ となる N が少なくとも1つあることが容易にわかる．このとき $n\geqq N$ をみたすすべての n に対し $|a_n|_p=|a_N|_p$ である．そこで $|\{a_n\}|_p=|a_N|_p$ と定義する．また $a_n\neq 0$ がすべての n に対し成り立てば，$\{a_n^{-1}\}\in\mathfrak{F}$ であることがわかる．

$\mathfrak{N}$ が極大イデアルであることを示そう．もしそうでなければ，$\mathfrak{M}$ という $\mathfrak{N}$ より真に大きいイデアルが存在する．このイデアルは $\mathfrak{N}$ に含まれない元 $\{a_n\}$ を含む．a_n のうち0であるものは有限個しかなく，それらを例えば1でおきかえるという操作は，$\{a_n\}$ に $\mathfrak{N}$ の元を加えることにほかならない．したがって，すべての n について $a_n\neq 0$ としてよい．すると，$\{a_n^{-1}\}\in\mathfrak{F}$ であり，$\{a_n^{-1}\}\{a_n\}\in\mathfrak{M}$ である．ゆえに $\mathfrak{M}=\mathfrak{F}$ となって矛盾である．したがって，$\mathfrak{N}$ は極大であり，$\mathfrak{F}/\mathfrak{N}$ は体である．

有理数体 $\boldsymbol{Q}$ は写像

$$r\to\{r\}\in\mathfrak{F}$$

により $\mathfrak{F}/\mathfrak{N}$ に埋め込まれる．$\mathfrak{F}$ 上の関数 $|\{a_n\}|$ は $\mathfrak{F}/\mathfrak{N}$ の付値で $\boldsymbol{Q}$ の像上では $|\ \ |_p$ に一致するものを与えるのは容易にわかる．

最後に，$\mathfrak{F}/\mathfrak{N}$ が完備であることは，$\mathfrak{F}$ の元の列に関する対角線論法により簡単に確かめられる．

【演習問題】

1　次の p, m, r に対し

$$|r-x|_p \leqq p^{-m}$$

をみたす $\boldsymbol{Z}$ の元 x を見つけるか，またはそのような x は存在しないことを示せ．

（i）　$p=257,\ r=1/2,\ m=1$

（ii）　$p=3,\ r=7/8,\ m=2$

（iii）　$p=3,\ r=7/8,\ m=7$

（iv）　$p=3,\ r=5/6,\ m=9$

（v）　$p=5,\ r=1/4,\ m=4$

2　問題 1 と同様なことを他の例について行なえ．

3　次の p, m, r に対し

$$|r-x^2|_p \leqq p^{-m}$$

をみたす $\boldsymbol{Z}$ の元 x を見つけるか，またはそのような x は存在しないことを示せ．

（i）　$p=5,\ r=-1,\ m=4$

（ii）　$p=5,\ r=10,\ m=3$

（iii）　$p=13,\ r=-4,\ m=3$

（iv）　$p=2,\ r=-7,\ m=6$

（v）　$p=7,\ r=-14,\ m=4$

（vi）　$p=7,\ r=6,\ m=3$

（vii）　$p=7,\ r=1/2,\ m=3$

4　問題 3 に関して問題 2 と同じことを行なえ．

5　p は $p\equiv 2\ (3)$ をみたす素数とする．p で割り切れない任意の整数 a に関し $x^3=a$ をみたす $\boldsymbol{Z}_p$ の元が存在することを示せ．

3

2 次曲線に関する局所–大域原理

すでにみたように，$\boldsymbol{Q}$ 上の種数 0 の曲線の有理点に関する問題は，与えられた 2 次曲線が有理点をもつか否かという問題に帰着された．

同次座標系を用いれば，$\boldsymbol{Q}$ 上定義された 2 次曲線 $\mathcal{C}$ は次の方程式で与えられる．

$$F(\boldsymbol{X}) = \sum f_{ij} X_i X_j = 0$$

ただし，$\boldsymbol{X} = (X_1, X_2, X_3)$，

$$f_{ij} = f_{ji} \in \boldsymbol{Q}$$

であり，2 次形式 F（**形式**とは，同次式のことである）は非特異，すなわち，

$$\det(f_{ij}) \neq 0$$

である．

最初の章で，実数の性質を使ったような議論を用いず，合同式を用いて有理点の非存在性を証明できることを述べた．ここでは，そこで p–進数を用いる．

2 次曲線上の有理点の存在に関する判定条件は Legendre により与えれたが，それを以下のように簡明な形に書き直したのは Hasse である．

定理 1　$\boldsymbol{Q}$ 上の 2 次曲線 $\mathcal{C}$ 上に有理点が存在するための必要十分条件は，$\mathcal{C}$ が実数体 $\boldsymbol{R}$ 上およびすべての素数 p に関し $\boldsymbol{Q}_p$ 上で定義された点をもつことである．　□

必要性は明白である．十分性を示していくが，それには多少の準備が必要

である．まず，慣例的な用語をいくつか導入しよう．

実数体 $\boldsymbol{R}$ はある意味で $\boldsymbol{Q}_p$ に類似しており，慣例的に $\boldsymbol{Q}_\infty$ と書く．$\boldsymbol{Q}_p$ と書いたときは，特に断らない限り $p=\infty$ は含まないものとする．体 $\boldsymbol{Q}_p$ は（$p=\infty$ も含めて）$\boldsymbol{Q}$ の局所化とよばれるが，これに対し $\boldsymbol{Q}$ は大域体とよばれる．何かが“局所的にいたるところで”正しいとは，その何かが $p=\infty$ を含めたすべての $\boldsymbol{Q}_p$ 上で正しいことをいう．このいい方を用いれば，定理 1 は“2 次曲線が大域点をもつ必要十分条件は，その 2 次曲線が局所的にいたるところで点をもつことである”となる．

2 次曲線に関する局所–大域定理から種数 0 の曲線に関する局所–大域定理が従うが，その定式化には少し注意が必要である（“点”は“座(place)”におきかえねばならない）．この件に関してはこれ以上立ち入らない．

この章の残りの部分では，定理 1 をより扱いやすい形にいいかえていく[*1]．

座標変換

$$T:\ X_i=\sum_i t_{ij}Y_j$$

ただし

$$t_{ij}\in\boldsymbol{Q},\quad \det(t_{ij})\neq 0$$

は 2 次形式 $F(\boldsymbol{X})$ を他の 2 次形式 $G(\boldsymbol{Y})$ にうつす．T は $F(\boldsymbol{X})=0$ の $\boldsymbol{Q}$ 上定義された点を $G(\boldsymbol{Y})=0$ の $\boldsymbol{Q}$ 上定義された点にうつす．また，同様に，T^{-1} は $G(\boldsymbol{Y})=0$ の $\boldsymbol{Q}$ 上定義された点を $F(\boldsymbol{X})=0$ の $\boldsymbol{Q}$ 上定義された点にうつす．各 p（$p=\infty$ を含めて）に対して $\boldsymbol{Q}_p$ 上定義された点に関しても同様である．したがって，定理 1 が $F(\boldsymbol{X})=0$ に関して正しいことと，$G(\boldsymbol{Y})=0$ に関して正しいこととは同値である．

このようにして適当な座標変換 T をとれば，“対角”形式

$$F(\boldsymbol{X})=f_1X_1^2+f_2X_2^2+f_3X_3^2$$

のみを扱えばよいことがわかる．さらに，$X_j\to t_jX_j$ $(t_j\in\boldsymbol{Q})$ とおきかえて一般性を失うことなく，

---

*1　定理 1 の証明の詳細には楕円曲線を使うことは必要ない．楕円曲線のみに興味をもつ読者は，この章の残りと第 4 章，第 5 章を省略してよい．

$$f_j \in \boldsymbol{Z}$$

は平方数で割り切れないとしてよい．

f_1, f_2, f_3 が共通因子 p をもてば $F(\boldsymbol{X})$ を $p^{-1}F(\boldsymbol{X})$ でおきかえる．また f_j のうち 2 つ，例えば f_1, f_2 が p で割り切れ，かつ $p \nmid f_3$ のときは，X_3 を pX_3 でおきかえれば F は p で割り切れるとしてよい．これらの操作を繰り返すことにより，$f_1f_2f_3$ の絶対値を小さくできる．そして，有限回の操作のあと，$f_1f_2f_3$ が平方数で割り切れない場合に帰着できる．こうして次の補題を得る．

補題 1　定理 1 を証明するには，2 次曲線

$$F(\boldsymbol{X}) = f_1X_1^2 + f_2X_2^2 + f_3X_3^2 = 0$$

で，$f_j \in \boldsymbol{Z}$ かつ $f_1f_2f_3$ は平方数で割り切れないものに関して証明すれば十分である．□

次のステップは，補題 1 の 2 次曲線が局所的にいたるところで解をもつという仮定から結論を導き出すことである．ベクトル $\boldsymbol{a} = (a_1, a_2, a_3) \neq (0,0,0)$　$(a_j \in \boldsymbol{Q}_p)$ が $F(\boldsymbol{a}) = 0$ をみたすならば，$\boldsymbol{Q}_p$ 上定義された点が得られる．a_j に $\boldsymbol{Q}_p$ の元をかけて一般性を失うことなく

$$\max |a_j|_p = 1 \qquad (*)$$

としてよい．いくつかの場合に分けて考える．

第 1 の場合 $(p \neq 2,\ p|f_1f_2f_3)$　一般性を失うことなく，$p|f_1$, $p \nmid f_2$, $p \nmid f_3$ と仮定してよい．すると $|f_1a_1^2|_p < 1$ である．ここで $|a_2|_p < 1$ と仮定しよう．すると

$$|f_3a_3^2|_p = |f_1a_1^2 + f_2a_2^2|_p < 1$$

であるから，$|a_3|_p < 1$ である．したがって

$$|f_1a_1^2|_p = |f_2a_2^2 + f_3a_3^2|_p \leqq p^{-2}$$

となり，f_1 は平方数で割り切れないから $|a_1|_p < 1$ であるが，これは$(*)$に反する．ゆえに $|a_2|_p = |a_3|_p = 1$ である．一方，

$$|f_2a_2^2 + f_3a_3^2|_p < 1$$

であるから，単数 a_2 で割って

$$f_2 + r_p^2 f_3 \equiv 0 \quad (p)$$

をみたす $\boldsymbol{Z}$ の元 r_p があるとしてよい．

第 2 の場合 ($p=2,\ 2\nmid f_1f_2f_3$)　a_j のうち単数であるのは 2 つのみであることは容易にわかる．それらを a_2, a_3 としよう．すると，$\boldsymbol{Z}$ の元 a は $a^2\equiv 1\ (4)$ または $a^2\equiv 0\ (4)$ をみたすから，

$$f_2+f_3\equiv 0 \quad (4)$$

を得る．

第 3 の場合 ($p=2,\ 2|f_1f_2f_3,\ 2|f_1$)　第 2 の場合と同様 $|a_2|_2=|a_3|_2=1$ としてよい．a が奇数ならば $a^2\equiv 1\ \ (8)$ であるから，$|a_1|_2<1$ ならば

$$f_2+f_3\equiv 0 \quad (8),$$

$|a_1|_2=1$ ならば

$$f_1+f_2+f_3\equiv 0 \quad (8)$$

を得る． □

続く 2 つの章で，上記の条件が $F(\boldsymbol{X})=0$ の大域点の存在を保証するのに十分であることを示す．

【演習問題】

1

(i)　p は奇素数，b, c は整数で b は p で割り切れないものとする．$x\in\boldsymbol{Z}$ に対し，bx^2+c は p を法としてちょうど $\dfrac{1}{2}(p+1)$ 個の相異なる値をとることを示せ．

(ii)　さらに，$a\in\boldsymbol{Z}$ かつ $p\nmid a$ と仮定する．このとき，$bx^2+c\equiv ay^2\ \ (p)$ をみたす整数 x, y が存在することを示せ．

2　p は奇素数とし，$a, b, c\in\boldsymbol{Z}_p$, $|a|_p=|b|_p=|c|_p=1$ とする．$bx^2+c=ay^2$ をみたす $x, y\in\boldsymbol{Z}_p$ が存在することを示せ．

3　p は奇素数，$a_{ij}\ (1\leqq i, j\leqq 3)$ は $a_{ji}=a_{ij}$ をみたす整数とし，$d=\det(a_{ij})$ とおく．$p\nmid d$ と仮定する．$\sum_{i,j} a_{ij}x_ix_j\equiv 0\ \ (p)$ をみたす整数 x_1, x_2, x_3 のうち少なくとも 1 つは p の倍数でないようなものが存在することを証明せよ．

4　$a, b, c\in\boldsymbol{Z}$, $2\nmid abc$ とする．$ax^2+by^2+cz^2=0$ が $\boldsymbol{Q}_2$ で自明な解しかもたないための必要十分条件は，$a\equiv b\equiv c\ \ (4)$ であることを示せ．

5　以下の (a, b, c) の組に対し，$ax^2+by^2+cz^2=0$ が $\boldsymbol{Q}_p$ で自明な解しかもた

ないような素数 p（∞ も含めて）の集合を求めよ．

（i）　$(a, b, c)=(1, 1, -2)$

（ii）　$(a, b, c)=(1, 1, -3)$

（iii）　$(a, b, c)=(1, 1, 1)$

（iv）　$(a, b, c)=(14, -15, 33)$

6　上記の計算で，自明な解がないような素数（∞ を含めて）の数 N に関して類似を認めたか？　もしそうでなければ，それがわかるまでその他の例を計算してみよ．

7

（i）　$a=1,\ b=-r,\ c=-s$ で r, s が異なる奇素数という特殊な場合に，前問で求めた類似性から類推される結果を証明せよ．

［ヒント．平方剰余の相互法則を用いる．］

（ii）　［難しい］一般の $a, b, c \in \boldsymbol{Z}$ に対して（i）と同じことを行なえ．

4

数の幾何学

ここで数の幾何学の手法が必要となるが，その初歩から始めよう．

引きだし論法の一般化によれば，N 個のものを H 個の引きだしに入れるとき，$N>mH$ (m は整数)なら，少なくとも 1 つの引きだしに $(m+1)$ 個のものが入っていなければならない．これの連続版の類似をまず考える．

$\boldsymbol{R}^n$ は $\boldsymbol{r}=(r_1,\cdots,r_n)$ からなる n 次元実ベクトル空間とする．このベクトル空間は群 $\boldsymbol{Z}^n$ を含む(すべての j について $r_j\in\boldsymbol{Z}$ となるような $\boldsymbol{r}$ 全体)．$\boldsymbol{R}^n$ の部分集合 $\mathcal{S}$ の体積 $V(\mathcal{S})$ はこのルベーグ測度を表すが，ここでは $\mathcal{S}$ は非常な素朴なもののみを扱う．

補題 1　m は正整数で $\mathcal{S}\subset\boldsymbol{R}^n$ は

$$V(\mathcal{S})>m$$

をみたすものとする．そのとき

$$\boldsymbol{s}_i-\boldsymbol{s}_j\in\boldsymbol{Z}^n \qquad (0\leqq i,j\leqq m)$$

をみたす $\mathcal{S}$ の $m+1$ の相異なる点 $\boldsymbol{s}_0,\cdots,s_m$ が存在する．

［証明］　部分集合 $\mathcal{W}\subset\boldsymbol{R}^n$ は“単位立方体”

$$\mathcal{W}=\{\boldsymbol{w}\in\boldsymbol{R}\mid 0\leqq w_j<1\ \ (1\leqq j\leqq n)\}$$

とする．するとすべての $\boldsymbol{x}\in\boldsymbol{R}^n$ は

$$\boldsymbol{x}=\boldsymbol{w}+\boldsymbol{z} \qquad (\boldsymbol{z}\in\boldsymbol{Z}^n)$$

という形に書ける．$\psi(\boldsymbol{x})$ は $\mathcal{S}$ の特性関数($\boldsymbol{x}\in\mathcal{S}$ ならば $\psi(\boldsymbol{x})=1$，$\boldsymbol{x}\notin\mathcal{S}$ ならば $\psi(\boldsymbol{x})=0$ という関数)とすれば，

$$m < V(\mathcal{S}) = \int_{\boldsymbol{R}^n} \psi(\boldsymbol{x})\,d\boldsymbol{x}$$
$$= \int_{\mathcal{W}} \left(\sum_{\boldsymbol{z} \in \boldsymbol{Z}^n} \psi(\boldsymbol{w}+\boldsymbol{z}) \right) d\boldsymbol{w}\,.$$

$V(\mathcal{W})=1$ であるから,

$$\sum_{\boldsymbol{z} \in \boldsymbol{Z}^n} \psi(\boldsymbol{w}_0+\boldsymbol{z}) > m$$

をみたす $\mathcal{W}$ の元 $\boldsymbol{w}_0$, すなわち, 左辺の値が $m+1$ 以上となるものが存在する. このとき, $\psi(\boldsymbol{w}_0+\boldsymbol{z})>0$ をみたす $\boldsymbol{w}_0+\boldsymbol{z}$ を $\boldsymbol{s}_j$ とおけばよい. ∎

集合 $\mathcal{S}$ が "$\boldsymbol{x}\in\mathcal{S}$ ならば $-\boldsymbol{x}\in\mathcal{S}$" をみたすとき, $\mathcal{S}$ は(原点に関し)**対称的**であるとよぶ. また $\boldsymbol{x}, \boldsymbol{y}\in\mathcal{S}$ に対し線分

$$\lambda\boldsymbol{x}+(1-\lambda)\boldsymbol{y} \in \mathcal{S} \qquad (0 \leqq \lambda \leqq 1)$$

が $\mathcal{S}$ に含まれるとき, **凸**であるとよぶ. 集合 $\mathcal{S}$ が凸ならば, 2 点 $\boldsymbol{x}, \boldsymbol{y}$ に関し中点 $\dfrac{1}{2}(\boldsymbol{x}+\boldsymbol{y})$ は $\mathcal{S}$ に含まれる.

定理 1 Λ は $\boldsymbol{Z}^n$ の指数 m の部分群とする. $\mathcal{C}$ は $\boldsymbol{R}^n$ の凸かつ対称的な部分集合で, 体積が

$$V(\mathcal{C}) > 2^n m$$

であるものとする. このとき, $\mathcal{C}$ と Λ は $\boldsymbol{0}=(0,\cdots,0)$ 以外に共通点をもつ.

［証明］ $\mathcal{S}=\dfrac{1}{2}\mathcal{C}$ を点 $\dfrac{1}{2}\boldsymbol{c}$ $(\boldsymbol{c}\in\mathcal{C})$ からなる集合とする. すると,

$$V\left(\frac{1}{2}\mathcal{C}\right) = 2^{-n}V(\mathcal{C}) > m$$

である. すると補題 1 から $m+1$ 個の相異なる点 $\boldsymbol{c}_0,\cdots,\boldsymbol{c}_m\in\mathcal{C}$ で

$$\frac{1}{2}\boldsymbol{c}_i - \frac{1}{2}\boldsymbol{c}_j \in \boldsymbol{Z}^n \qquad (0 \leqq i, j \leqq m)$$

をみたすものがとれる. すなわち, $m+1$ 個の点

$$\frac{1}{2}\boldsymbol{c}_i - \frac{1}{2}\boldsymbol{c}_0 \qquad (0 \leqq i \leqq m)$$

があり, Λ の $\boldsymbol{Z}^n$ の剰余類の数は m であるから, 引きだし論法によりこのうちの 2 点は同じ剰余類に属さねばならない. つまり,

$$\frac{1}{2}\boldsymbol{c}_i - \frac{1}{2}\boldsymbol{c}_j \in \Lambda$$

をみたす相異なる $\boldsymbol{c}_i, \boldsymbol{c}_j\ (i \neq j)$ がある．$\mathcal{C}$ は対称的であるから $-\boldsymbol{c}_j \in \mathcal{C}$ であり，凸性から

$$\frac{1}{2}\boldsymbol{c}_i - \frac{1}{2}\boldsymbol{c}_j = \frac{1}{2}\boldsymbol{c}_i + \frac{1}{2}(-\boldsymbol{c}_j) \in \mathcal{C}$$

である．▮

注意　$m=1$ のとき補題 1 は Blichfeldt，定理 1 は Minkowski による．$m>1$ のときの一般化は van der Corput による．

次の章でこの章の結果をどのように応用するか，その雰囲気を前もって味わってもらうため，次の補題を証明しよう．

補題 2　N は正整数とする．

$$l^2 \equiv -1 \quad (N)$$

をみたす整数 l が存在すれば，$N = u^2 + v^2$ をみたす整数 u, v が存在する．

［証明］　$n=2$ とし，座標を x, y で表す．$\mathcal{C}$ として開円盤

$$x^2 + y^2 < 2N$$

をとれば，体積（この場合は面積）は

$$V(\mathcal{C}) = 2\pi N > 2^2 N$$

である．$\boldsymbol{Z}$ の部分群 Λ を

$$x, y \in \boldsymbol{Z}, \quad y \equiv lx \quad (N)$$

で定義すれば，指数は N である．したがって，定理 1 から $(0,0)$ と異なる (u,v) で

$$(u,v) \in \Lambda \cap \mathcal{C}$$

をみたすものがある．

$$0 < u^2 + v^2 < 2N$$

かつ

$$u^2 + v^2 \equiv u^2(1 + l^2) \equiv 0 \quad (N)$$

であるから，$u^2 + v^2 = N$ を得る．▮

補題 2 の条件は $p \equiv 1\ (4)$ をみたす素数 p に関して確かにみたされること

を示すことは読者にまかせよう.

【演習問題】

1　整数 $m>1$ に対し，$f^2+f+1\equiv 0\ \ (m)$ をみたす整数 f が存在するとする. このとき $m=u^2+uv+v^2$ をみたす整数 u, v が存在することを示せ.

2

$$1+5f^2\equiv 0 \quad (p)$$

をみたす整数 f は存在するが，$p=u^2+5v^2$ (u, v は整数) という形には書けない素数 p を見つけよ.

5

局所–大域原理(証明の完結)

さて，前章の定理を用いて 2 次曲線に関する局所–大域原理を証明しよう．まず，次の形の 2 次曲線に対して証明すればよかったことを思い出そう．

$$f_1X_1^2+f_2X_2^2+f_3X_3^2=0$$

ただし，f_1, f_2, f_3 は整数で $f_1f_2f_3$ は平方数で割り切れないものとする．この 2 次曲線が局所的にいたるところで解をもつと仮定し，それが $2f_1f_2f_3$ を割り切るいくつかの素数 p の合同条件になることを示そう．

まず，$\boldsymbol{Z}^3$ の部分群 Λ を，$\boldsymbol{x}=(x_1, x_2, x_3)$ の各成分に以下の合同条件を課すことで定義しよう．

第 1 の場合 $(p\neq 2,\ p|f_1f_2f_3,\ p|f_1)$　第 3 章の終りでみたように

$$f_2+r_p^2f_3\equiv 0 \quad (p)$$

をみたす整数 r_p が存在する．条件

$$x_3\equiv r_px_2 \quad (p)$$

を課せば

$$\begin{aligned} F(\boldsymbol{x}) &= f_1x_1^2+f_2x_2^2+f_3x_3^2 \\ &\equiv (f_2+r_p^2f_3)x_2^2 \\ &\equiv 0 \quad (p). \end{aligned}$$

第 2 の場合 $(p=2,\ 2\nmid f_1f_2f_3)$　一般性を失うことなく

$$f_2+f_3\equiv 0 \quad (4)$$

としてよい．条件

$$\begin{cases} x_1 \equiv 0 \quad (2), \\ x_2 \equiv x_3 \quad (2) \end{cases}$$

を課せばこれから

$$F(\boldsymbol{x}) \equiv 0 \quad (4)$$

が従う．

第 3 の場合 $(p=2,\ 2|f_1f_2f_3,\ 2|f_1)$　このとき

$$s^2f_1+f_2+f_3 \equiv 0 \quad (8)$$

（s は 0 または 1）となる．これに条件

$$\begin{cases} x_2 \equiv x_3 \quad (4), \\ x_1 \equiv sx_3 \quad (2) \end{cases}$$

を課せばこれから

$$F(\boldsymbol{x}) \equiv 0 \quad (8)$$

が従う．　□

以上をまとめると，$\boldsymbol{Z}^3$ の部分群 Λ の指数 $m=4|f_1f_2f_3|$（$|\quad|$ はこの章では絶対値を表すと仮定しておく）である．さらに，$\boldsymbol{x}\in\Lambda$ に対し

$$F(\boldsymbol{x}) \equiv 0 \quad (4|f_1f_2f_3|)$$

が成立する．

前章の定理を Λ と凸な対称的集合

$$\mathcal{C}:\ |f_1|x_1^2+|f_2|x_2^2+|f_3|x_3^2 < 4|f_1f_2f_3|$$

に適用してみよう．容易にわかるように

$$\begin{aligned} V(\mathcal{C}) &= \frac{\pi}{3}\cdot 2^3\cdot|4f_1f_2f_3| \\ &> 2^3\,|4f_1f_2f_3| \\ &= 2^3m \end{aligned}$$

である．したがって $(0,0,0)$ でない $\Lambda\cap\mathcal{C}$ の元 $\boldsymbol{x}$ が存在する．この $\boldsymbol{x}$ を用いれば

$$F(\boldsymbol{x}) \equiv 0 \quad (4|f_1f_2f_3|)$$

かつ

$$|F(\boldsymbol{x})| \leqq |f_1|x_1^2+|f_2|x_2^2+|f_3|x_3^2$$
$$< 4\,|f_1f_2f_3|$$

であるから

$$F(\boldsymbol{x}) = 0$$

を得る.

いくつかの注意をしてこの章を終えよう.

注意 1 上記の証明は単に $F(\boldsymbol{x})=0$ の解の存在を証明しただけでなく，その解がある楕円体の中に存在することを示している．これは具体的な場合に解を求めるのに有効である.

注意 2 $p\nmid 2f_1f_2f_3$ なる素数 p について $\boldsymbol{Q}_p$ で解があるということは用いてない．実際，この条件は何の情報をもたらさない（第 3 章演習問題 2, 3 を参照）．任意の f_1, f_2, f_3 と $p\nmid 2f_1f_2f_3$ なる素数 p に対して

$$f_1X_1^2+f_2X_2^2+f_3X_3^2=0$$

が $\boldsymbol{Q}_p$ で解をもつことを示すことは読者にまかせよう.

注意 3 $\boldsymbol{Q}_\infty=\boldsymbol{R}$ での解の存在も用いてない.

したがって $\boldsymbol{Q}_\infty$ での解の存在は他のすべての $\boldsymbol{Q}_p$ $(p\neq\infty)$ での解の存在から従う．この事実は平方剰余の相互法則と関係している．実際，$\boldsymbol{Q}$ 上の任意の 2 次曲線について，$\boldsymbol{Q}_p$ で解がないような p（∞ も含めて）の数は偶数である（第 3 章演習問題 6, 7 参照）．2 次形式の本（例えば著者のものなど）を参照のこと.

【演習問題】

1 $$F(X,Y,Z)=5X^2+3Y^2+8Z^2+6(YZ+ZX+XY)$$

に対して，

$$F(x,y,z)\equiv 0 \pmod{13^2}$$

をみたす有理整数 x,y,z で少なくとも 1 つは 13 の倍数でないものを見つけよ.

［ヒント．第 10 章の Hensel の補題を参照.］

2 $$F(X,Y,Z)=7X^2+3Y^2-2Z^2+4YZ+6ZX+2XY$$

に対して,

$$F(x,y,z)\equiv 0 \pmod{17^3}$$

をみたす有理整数 x,y,z で少なくとも 1 つは 17 の倍数でないものを見つけよ.

6

3 次曲線

この章では，3 次形式

$$\mathcal{C}:\ F(\boldsymbol{X}) = F(X_1, X_2, X_3) = 0$$

で与えられた曲線を考える．興味があるのは基礎体が $\boldsymbol{Q}$ のときであるが，最初に述べることは一般の基礎体に対しても適用できる．

$\mathcal{C}$ 上の点 $\boldsymbol{x}$ が

$$\frac{\partial F}{\partial X_j}(\boldsymbol{x}) = 0 \qquad (j = 1, 2, 3)$$

をみたすとき，$\boldsymbol{x}$ は**特異**であるとよばれる．座標を $\boldsymbol{x} = (0, 0, 1)$ となるようにとれば F が X_3^3, $X_1X_3^2$, $X_2X_3^2$ という項を含まないことと同値である．

特異点では直線と重複度を込めて少なくとも 2 回以上交わる．より正確には，$\boldsymbol{a}$, $\boldsymbol{b}$ を直線上の 2 点とすれば，この直線上の点は

$$\lambda\boldsymbol{a} + \mu\boldsymbol{b}$$

（ただし λ, μ の一方は 0 でないとする）と表される．この直線と $\mathcal{C}$ との交点は λ, μ に関する同次 3 次式

$$F(\lambda\boldsymbol{a} + \mu\boldsymbol{b}) = 0 \qquad (*)$$

で与えられる．交点の 1 つが $\mathcal{C}$ の特異点であるとは，比 $\lambda : \mu$ が$(*)$の重複解となっていることである．これを確かめるには $\boldsymbol{b} = \boldsymbol{x}$ とおいてみればよい．

$\mathcal{C}$ が相異なる 2 つの特異点 $\boldsymbol{x}$, $\boldsymbol{y}$ をもったとしよう．$\boldsymbol{x}$, $\boldsymbol{y}$ を通る直線は $\mathcal{C}$ と $\boldsymbol{x}$, $\boldsymbol{y}$ で重複度が 2 以上で交わる．これは $F(\lambda\boldsymbol{x} + \mu\boldsymbol{y})$ が恒等的に 0 になる

とき，つまり$\mathcal{C}$が直線を含むときに限って起こる．したがって，$\mathcal{C}$は**既約**(Fは因数分解できない)と仮定すればこのようなことは起きない．ゆえに，既約な3次曲線は特異点をたかだか1つしかもたないことがわかる．

基礎体が$\boldsymbol{Q}$であるとしよう．代数閉包$\overline{\boldsymbol{Q}}$上で特異点があればそれはたかだか1つである．ガロア理論*1を使えばそれは$\boldsymbol{Q}$上定義されていなければならないことがわかる．したがって，第1章でみたように，$\mathcal{C}$は$\boldsymbol{Q}$上直線に双有理同値である．

これからは**非特異**3次曲線，すなわち$\boldsymbol{Q}$上で特異点をもたない3次曲線のみを考える．$\boldsymbol{a}$, $\boldsymbol{b}$を$\mathcal{C}$上の有理点とする．これらを結ぶ直線は一般には異なる3番目の点で交わる．その点はまた有理点である．なぜなら，その点は3つの解のうち2つが有理数であるような3次方程式の解から得られるからである．この論法の変形で，すでにわかっている有理点から新しいものを得る方法として，有理点における接線との3番目の交点をとるものがあるが，これはすでにDiophantosにより使われていたようである．一般的な方法はWeilによると最初にニュートンが指摘したそうである．古い世代の数学者はこの方法を“弦と接線の方法(chord and tangent process)”とよんでいる．

一般に弦と接線の方法を用いれば，$\mathcal{C}$上の有理点$\boldsymbol{a}$から出発して無限個の有理点が得られる．無限個の点が得られないとき$\boldsymbol{a}$は**例外的**とよばれる．例外点については，例えば次の補題が成り立つ．

補題1　3乗の因子を含まない整数$a\geqq 1$と，3次曲線$\mathcal{C}$

$$\mathcal{C}:\ X^3+Y^3-aZ^3=0$$

を考える．このとき点$(1,-1,0)$は例外的である．$a=1$のときは点$(0,1,1)$, $(1,0,1)$も例外的である．また$a=2$のときは$(1,1,1)$も例外点である．これら以外に例外点はない．

［証明］　まず上記の点が確かに例外点であることを示そう．点$(1,-1,0)$における接線は$X+Y=0$であり，それは$\mathcal{C}$と$(1,-1,0)$でのみ交わる．$a=1$のときは他の点も同様である．$a=2$のとき$(1,1,1)$での接線は$X+Y-$

*1　進んだ読者のために：基礎体が完全体でないときはこの結論は必ずしも成立しない．第9章の最後を参照．

$2Z=0$ であり，$\mathcal{C}$ とは $(1,-1,0)$ で交わる．

$\boldsymbol{x}=(x,y,z)$ は上にあげた点以外の有理点としよう．x, y, z は互いに素と仮定してよい．すると，$\mathcal{C}$ の定義方程式から x, y, z は 2 つずつが互いに素となる．

$\boldsymbol{x}_1=(x_1,y_1,z_1)$ は 3 番目の交点とする．ここで x_1, y_1, z_1 はまた共通因子をもたない整数である．さらに

$$x_1 : y_1 : z_1 = x(x^3+2y^3) : -y(2x^3+y^3) : z(x^3-y^3)$$

という関係があることがわかる[*2]．

d を右辺の 3 項の最大公約数としよう．素数 p が x と d を共に割り切れば y も割り切ることになり矛盾．したがって，d は x^3+2y^3 または $2x^3+y^3$ を割り切らねばならない．つまり，$3x^3$ と $3y^3$ を割り切ることになり，$d=1$ または 3 となる．ゆえに

$$z_1 = \pm z(x^3-y^3) \quad \text{または} \quad z_1 = \pm z(x^3-y^3)/3$$

を得る．いずれの場合にも，$\boldsymbol{x}$ が補題で述べたものでなければ $|z_1|>|z|$ をみたすことがわかる．接線を繰り返し用いて

$$|z| < |z_1| < |z_2| < \cdots$$

をみたす点列 $\boldsymbol{x}, \boldsymbol{x}_1, \boldsymbol{x}_2, \cdots$ を得る．これらの点はすべて異なっており，したがって $\boldsymbol{x}$ が例外的でないことが示された．∎

【演習問題】

1

（i）
$$4A^3+27B^2 \neq 0$$

ならば，3 次曲線

$$Y^2Z = X^3+AXZ^2+BZ^3$$

は非特異であることを示せ．

（ii）　$4A^3+27B^2=0$ のとき特異点を求め，それが尖点(cusp)か異なる接線を

---

*2　これは Desboves の “弦と接線の方法” に関するエレガントな公式の特別な場合である．演習問題と公式集参照．

もつ 2 重点であるかを決定せよ．

2

（i）
$$F(\boldsymbol{X})=a_1X_1^3+a_2X_2^3+a_3X_3^3+dX_1X_2X_3$$

ただし

$$a_1a_2a_3\neq 0$$

とおく．

$$27a_1a_2a_3+d^3\neq 0$$

ならば $F(\boldsymbol{X})=0$ は非特異であることを示せ．

（ii） $a_1=a_2=a_3=1$, $d=-3$ ならば $x_1^3=x_2^3=x_3^3=x_1x_2x_3=1$ をみたす任意の点は特異点であることを示せ．

（iii） 前問の結果はこの章で証明した 3 次曲線はたかだか 1 つしか特異点をもたないという結果となぜ矛盾しないか考えよ．

3 $F(\boldsymbol{X})$ は前問の通りとし，$F(\boldsymbol{X})=0$ は非特異とする．

（i） $F(\boldsymbol{x})=0$ とする．$\boldsymbol{x}$ における接線との 3 番目の交点 $\boldsymbol{t}$ は

$$t_j=x_j(a_{j+1}x_{j+1}^3-a_{j+2}x_{j+2}^3)\qquad (j=1,2,3)$$

（ただし添え字は 3 を法として考える）で与えられる．

（ii） $\boldsymbol{x}$, $\boldsymbol{y}$ は $F(\boldsymbol{X})=0$ 上の相異なる 2 点とする．この 2 点を結ぶ直線との 3 番目の交点 $\boldsymbol{z}$ は

$$z_j=x_j^2y_{j+1}y_{j+2}-y_j^2x_{j+1}x_{j+2}$$

で与えられる．（Desboves の公式）

4 $X^3+Y^3+7Z^3=0$ の解 $(2,-1,-1)$ から出発して相異なる 10 個の解を求めよ．

7

非特異 3 次曲線と群構造

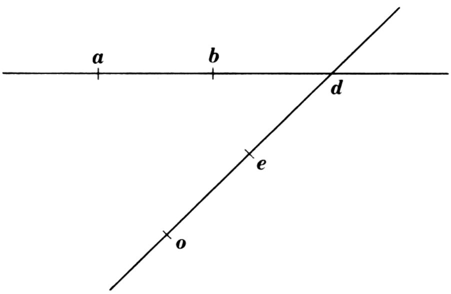
$\mathcal{C}$ は非特異 3 次曲線とし，$\boldsymbol{o}$ は $\mathcal{C}$ 上の有理点とする．$\mathcal{C}$ 上の有理点全体の集合に $\boldsymbol{o}$ (“ゼロ”)を単位元とする自然な可換群の構造が入ることを示そう．

ここでは基礎体は任意とし，曲線 $\mathcal{C}$ はその体上定義されているものとする．そして有理点はその基礎体上定義された点を表すものとする．

群の演算は以下のようにして定義される．$\boldsymbol{a}, \boldsymbol{b}$ は有理点とし，$\boldsymbol{d}$ は $\boldsymbol{a}, \boldsymbol{b}$ を通る直線が $\mathcal{C}$ と交わる 3 番目の点とする．さらに $\boldsymbol{e}$ は $\boldsymbol{o}, \boldsymbol{d}$ を通る直線が $\mathcal{C}$ と交わる 3 番目の点とする．このとき和を

$$\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{e}$$

と定義する．



この定義は，でてくる点のうち 2 点もしくはそれ以上が一致しているときには適当に定義しなおすことにする．例えば，$\boldsymbol{b}=\boldsymbol{a}$ ならば $\boldsymbol{a}$ における接線

を考える．

この演算 "+" が可換群の構造を与えることを示そう．明らかに

$$\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{b}+\boldsymbol{a}$$

であり，すべての $\boldsymbol{a}$ に関して

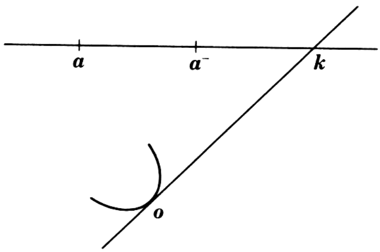
$$\boldsymbol{o}+\boldsymbol{a}=\boldsymbol{a}$$

である．

次に $\boldsymbol{a}$ の逆元を構成しよう．$\boldsymbol{o}$ における接線との 3 番目の交点を $\boldsymbol{k}$ とする．$\boldsymbol{a}^-$ を $\boldsymbol{a}$ と $\boldsymbol{k}$ を通る直線との 3 番目の交点とする．すると定義により，

$$\boldsymbol{a}+\boldsymbol{a}^-=\boldsymbol{o}$$

である．



ここで難しいのは + が結合法則をみたすこと，つまり

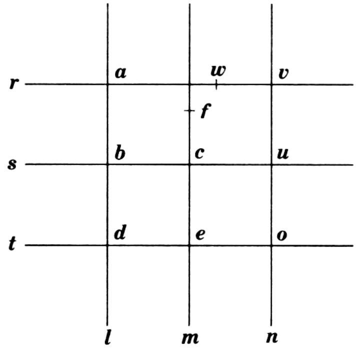
$$(\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c}=\boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c})$$

を示すことである．ここでは 2 通りの証明をする．最初のものは射影幾何学的であり，2 番目のものはより代数幾何学的なものである．

$\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ が与えられたとする．次の図を考えよう．

ここで $\boldsymbol{r}$, $\boldsymbol{s}$, $\boldsymbol{t}$, $\boldsymbol{l}$, $\boldsymbol{m}$, $\boldsymbol{n}$ は直線を表し，残りの記号は $\mathcal{C}$ 上の点を表す．$\boldsymbol{f}$, $\boldsymbol{w}$ 以外はすべて 2 つの直線の交点である．またこの図は $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, $\boldsymbol{o}$ が与えられれば決まるものである．

$(\boldsymbol{a}+\boldsymbol{b})=\boldsymbol{e}$ であり，したがって $(\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c}$ は $\boldsymbol{o}$, $\boldsymbol{f}$ を通る直線との 3 番目の交点である．同様に $\boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c})$ は $\boldsymbol{o}$, $\boldsymbol{w}$ を通る直線との 3 番目の交点である．ゆえに結合性を証明するには，$\boldsymbol{f}$, $\boldsymbol{w}$ が図のように相異なる点ではなく，直線 $\boldsymbol{r}$ と $\boldsymbol{m}$ の交点に一致していることを示さねばならない．



ここで次の補題を思い出そう．

補題 1　$\boldsymbol{x}_1, \cdots, \boldsymbol{x}_8$ は一般の位置[*1]にある平面上の 8 点とする．すると，次の性質をみたす 9 番目の点 $\boldsymbol{y}$ が存在する：　$\boldsymbol{x}_1, \cdots, \boldsymbol{x}_8$ を通るすべての 3 次曲線はまた $\boldsymbol{y}$ を通る．□

この補題の証明の概略を簡単に述べよう．3 次形式 $F(\boldsymbol{X})$，$\boldsymbol{X}=(X_1, X_2, X_3)$ には 10 個の係数がある．方程式 $F(\boldsymbol{X})=0$ は係数に線型な条件を 1 つ課す．$\boldsymbol{x}_1, \cdots, \boldsymbol{x}_8$ を通るという条件は 8 つの線型な条件を課す．ゆえに $F_1(\boldsymbol{X})$，$F_2(\boldsymbol{X})$ を 8 点を通る 1 次独立な 3 次形式とすれば，他の任意の F は

$$F(\boldsymbol{X}) = \lambda F_1(\boldsymbol{X}) + \mu F_2(\boldsymbol{X})$$

という形に書ける．$F_1=0$，$F_2=0$ は 9 点で交わり，$F=0$ がそれらすべてを通るのは明らかである．

さてこの補題を $\boldsymbol{f}=\boldsymbol{w}$ を証明するのに応用する．直線 $\boldsymbol{l}$ の方程式を $l(\boldsymbol{X})=0$ とおく（その他の直線についても同様である）．2 つの 3 次曲線

$$F_1(\boldsymbol{X}) = l(\boldsymbol{X})m(\boldsymbol{X})n(\boldsymbol{X}) = 0$$
$$F_2(\boldsymbol{X}) = r(\boldsymbol{X})s(\boldsymbol{X})t(\boldsymbol{X}) = 0$$

を考える．非特異な 3 次曲線 C は $F_1=0$ と $F_2=0$ の交点のうち 8 点を通る．したがって，補題から 9 番目の点を通らねばならない．よって $\boldsymbol{f}=\boldsymbol{w}$ を得

*1　この場合は，“どの 4 点も同一直線上になく，またどの 7 点も 1 つの 2 次曲線上にない” ということ．

る.

さて“+”の結合性に関する2つめの証明を与えよう.

1次形式, 例えば $l(\boldsymbol{X})$ は斉次的なので $\mathcal{C}$ 上の関数ではない. 一方, $t(\boldsymbol{X})$ をもう1つの1次形式とすれば, 商

$$g(\boldsymbol{X}) = l(\boldsymbol{X})/t(\boldsymbol{X})$$

は $\mathcal{C}$ 上の(有理)関数を定義する. いま述べた状況のもとで, $l(\boldsymbol{X})=0$ は $\mathcal{C}$ 上の点 $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{d}$ を通り, $t(\boldsymbol{X})=0$ は $\mathcal{C}$ 上の点 $\boldsymbol{d}, \boldsymbol{o}, \boldsymbol{e}$ を通る. こうして関数 $g(\boldsymbol{X})$ は零点 $\boldsymbol{a}, \boldsymbol{b}$, 極 $\boldsymbol{o}, \boldsymbol{e}$ をもつ. $\boldsymbol{d}$ は分母分子で打ち消し会うので, 零点でも極でもない.

代数曲線の非特異な点では1変数有理関数の零点や極の概念を一般化できるが, それをこの場合に適用すると, $g(\boldsymbol{X})$ は $\boldsymbol{a}, \boldsymbol{b}$ で1位の零点, $\boldsymbol{o}, \boldsymbol{e}$ で1位の極をもつということであり, 等式 $\boldsymbol{e}=\boldsymbol{a}+\boldsymbol{b}$ はこのような関数の存在と同値である.

同様に, 等式

$$\boldsymbol{x} = (\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c}$$

は $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ で1位の極をもち, $\boldsymbol{o}$ で2位の零点, $\boldsymbol{x}$ で1位の零点をもつ関数の存在と同値である. こうなると, 等式

$$(\boldsymbol{a}+\boldsymbol{b})+\boldsymbol{c} = \boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c})$$

は明らかである.

このようにして, 群の演算は曲線の関数体によっており, 双有理同値で不変であることがわかる. 代数幾何学では因子 $\{\boldsymbol{a}, \boldsymbol{b}\}$ が因子 $\{\boldsymbol{o}, \boldsymbol{c}\}$ に線型同値であるときに $\boldsymbol{a}+\boldsymbol{b}=\boldsymbol{c}$ であるという.

非特異3次曲線の種数が1とはどういうことかを簡単に説明してこの章を終えよう. $r \geqq 2$ とし, $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_r$, $\boldsymbol{y}_1, \cdots, \boldsymbol{y}_{r-1}$ は $\mathcal{C}$ 上の点とする. 簡単のためこれらの点はすべて相異なるとしよう. すると $g(\boldsymbol{X})$ を構成したように, 1次形式をうまく使って曲線上の関数 $h(\boldsymbol{X})$ で $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_r$ でのみ1位の極をもち, $\boldsymbol{y}_1, \cdots, \boldsymbol{y}_{r-1}$ で零点をもつ関数を構成できる. $h(\boldsymbol{X})$ はもう1つ零点をもつが, それは完全に決まってしまう.

直線のときと対比させてみよう. $c_1, \cdots, c_r$, $d_1, \cdots, d_r$ を任意の相異なる $2r$

個の数としよう．すると，関数

$$\prod_j (T-d_j) \Big/ \prod_j (T-c_j)$$

は d_j で 1 位の零点，c_j で 1 位の極をもち，それ以外には(無限遠においてさえ)零点も極ももたない．

曲線の種数とは関数に零点や極をどれくらいの自由度でもたせられるかをみる尺度である．本書では必要ではないが，正確に記述したものは少し複雑で，それは Riemann–Roch の定理とよばれるものである．

【演習問題】

1　$\boldsymbol{o}, \boldsymbol{a}$ は非特異 3 次曲線 $\mathcal{C}$ 上の有理点とする．$\boldsymbol{o}$ を群の単位元として $-\boldsymbol{a}$ を構成せよ．

2　$\boldsymbol{o}, \boldsymbol{o}_1$ は非特異 3 次曲線 $\mathcal{C}$ 上の有理点とする．$\boldsymbol{o}_1$ を単位元として得られる群演算は $\boldsymbol{o}$ を単位元として得られる群演算を用いてどのように記述されるかを調べよ．

3　$\boldsymbol{o}, \boldsymbol{a}$ は非特異 3 次曲線 $\mathcal{C}$ 上の有理点で，$\boldsymbol{o}$ を単位元とする群演算に関し $3\boldsymbol{a}=\boldsymbol{o}$ をみたす点とする．$\boldsymbol{b}=2\boldsymbol{a}$ とおく．3 角形 $\boldsymbol{o}, \boldsymbol{a}, \boldsymbol{b}$ の各辺ともう 1 つの頂点における接線との交点は $\mathcal{C}$ 上にあることを示せ．点 $\boldsymbol{o}, \boldsymbol{a}, \boldsymbol{b}$ がいま述べた 3 角形の頂点であるための条件を，$\mathcal{C}$ を定義する 3 次形式の係数を用いて表せ．

4　$\mathcal{C}$ は曲線

$$X^3+Y^3-XZ^2-YZ^2+7XYZ=0$$

とし，$\boldsymbol{x}=(x,y,z)$ は $\boldsymbol{Q}_p$ 上定義された $\mathcal{C}$ の有理点とする．p–進位相に関し，$\boldsymbol{x}\to(0,0,1)$ のとき $y/x\to -1$ であることを示せ．

5　この問題ではすべて $\boldsymbol{Q}_p$ 上定義されていると仮定する．$\boldsymbol{a}$ は 3 次曲線

$$F(X,Y,Z)=0$$

上の非特異な点とし，$t(\boldsymbol{X})=0$ はその点での接線とする．$l(\boldsymbol{X})=0,\ m(\boldsymbol{X})=0$ は $\boldsymbol{a}$ を通る接線と異なる直線とする．

$$dl(\boldsymbol{X})+em(\boldsymbol{X})+ft(\boldsymbol{X})=0$$

を恒等的にみたす d, e, f $(d\neq 0,\ e\neq 0)$ が存在することを示せ．p–進位相に関し，

$\boldsymbol{x} \to \boldsymbol{a}$ のとき

$$m(\boldsymbol{x})/l(\boldsymbol{x}) \to -d/e$$

であることを示せ.

8

楕円曲線とその標準形

基礎体上定義された代数曲線を双有理同値を法として考えると，種数が0のときは常に2次曲線または直線に双有理同値であった．種数が1のときはそのような特殊な形に帰着させることは不可能であるが，基礎体上定義された点（“有理点”）があると状況は変わってくる．このような場合に対して特別な名前をつけておくと便利である： 有理点を1つもつ種数1の曲線を**楕円曲線**とよぶ．

標準形として

$$\mathcal{C}:\ Y^2 = X^3 + AX + B$$

または同次座標を用いて

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

をとる．右辺は

$$4A^3 + 27B^2 \neq 0$$

ならば重複根をもたない．与えられた有理点 $\boldsymbol{o}$ は無限遠点 $(X, Y, Z) = (0, 1, 0)$ である．

無限遠直線は $\boldsymbol{o}$ で3重に接するので $\mathcal{C}$ 上の群演算は単純である：

$$-(x, y) = (x, -y)$$

であり，$\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ が同一直線上にあるときに限り $\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}=\boldsymbol{o}$ である．

基礎体が有理数体であるときはこの標準形のとりかたが特に便利であることがわかるであろう．基礎体の標数が2または3であるときは，$\mathcal{C}$ の標準形

はこのようにはとれず，

$$Y^2+a_1XY+a_3Y = X^3+a_2X^2+a_4X+a_6$$

という形のものをとらねばならないが，これは本書の目的にとってはあまり重要でないので，そのような場合を扱うのは読者にまかせることにしよう．

楕円曲線の定義をきちんとしたわけではないので，すべての楕円曲線が上の標準形で与えられるものに双有理同値であることの厳密な証明はしない．そのかわり，ある種の楕円曲線を標準形に変形するアルゴリズムを詳しく述べよう．初めての読者はここをとばしてもよい．

事実（標数$\neq 2,3$）　任意の楕円曲線は適当な A, B を係数とする標準形に基礎体上双有理同値である．

より正確にいうと，曲線は$\mathcal{C}$ に同値であり，与えられている有理点$\boldsymbol{O}$ はこの同値により$\mathcal{C}$ 上の無限遠点に対応する．

［証明］（進んだ読者向け）　Riemann–Roch の定理により，$\boldsymbol{O}$ でたかだか 2 位の極しかもたない曲線上の関数の集合は 2 次元である．その基底を $1, \xi$ としよう．同様に，$\boldsymbol{O}$ でたかだか 3 位の極しかもたない曲線上の関数の集合は 3 次元である．その基底を $1, \xi, \eta$ としよう．すると関数

$$\eta^2,\ \eta\xi,\ \eta,\ \xi^3,\ \xi^2,\ \xi,\ 1$$

はすべて $\boldsymbol{O}$ でたかだか 6 位の極しかもたない．Riemann–Roch の定理からこれらの 7 つの関数には 1 次従属でなければならない．また，その関係式は ξ^3, η^2 を共に含んでなければならない．ここで

$$\xi \to c_1\xi+c_2$$
$$\eta \to c_3\eta+c_4\xi+c_5$$

という形の変換を使えば適当な A, B を用いて関係式を

$$\eta^2 = \xi^3+A\xi+B$$

の形に帰着できる．　∎

進んだ読者向けの注意　種数 1 の曲線がなぜ標準形をもたないか，もしくは無限個の標準形をもつのかという理由は，$g=1$ ならば

$$2(g-1)=0$$

となることにある．他の種数の曲線については双有理写像を与えるのに基礎体上

定義された関数の微分の因子を用いることができる．例えば，種数 2 の曲線は常に $Y^2 =$ “X に関する 6 次式” という形の曲線に双有理同値である．

いくつかの特別な場合　上記の証明は実用的なアルゴリズムを与えてはいない．特殊な場合をいくつか考えよう．ここでは $\mathcal{C}$ の形にさえ変形できれば十分であることに注意しておく．というのは，もし有理点 $\boldsymbol{O}$ が $\boldsymbol{a}$ にうつされるなら，$\mathcal{C}$ 上で $\boldsymbol{x} \to \boldsymbol{x} - \boldsymbol{a}$ とおきかえればよいからである．

（i）　**3 次曲線 $\mathcal{D}$．有理点 $\boldsymbol{O}$ が変曲点のとき**

このときは $\boldsymbol{O}$ を $\boldsymbol{o}$，$\boldsymbol{O}$ での接線を無限遠直線にうつす線型な座標変換を考えれば十分である．

例えば，

$$\mathcal{D}:\ X^3 + Y^3 + dZ^3 = 0,$$
$$\boldsymbol{O} = (1, -1, 0)$$

のときは

$$X = U + V, \quad Y = U - V$$

とおけば

$$6UV^2 = -2U^3 - dZ^3,$$

ゆえに

$$Y_1^2 Z_1 = X_1^3 - 2^4 \cdot 3^3 \cdot d^2 Z_1^3$$

を得る．ここで

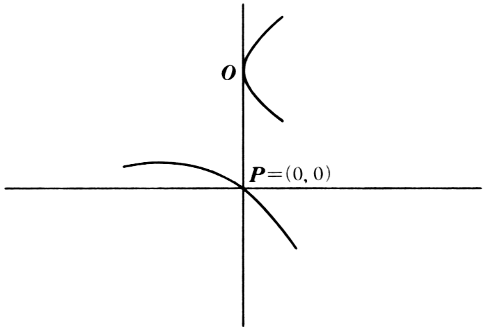
$$X_1 = -6dZ, \quad Y_1 = 6^2 dV, \quad Z_1 = U$$

である．

（ii）　**3 次曲線 $\mathcal{D}$．有理点 $\boldsymbol{O}$ が変曲点でないとき**[*1]

$\boldsymbol{O}$ における接線は $\mathcal{D}$ とまた有理点で交わる．この点を $\boldsymbol{P}$ としよう．$\boldsymbol{P}$ を原点とし $\boldsymbol{O}$ での接線を Y–軸とするアフィン座標をとる．

＊1　この論法は Nagell による：Sur les propriétés arithmétiques des cubiques planes du premier genre. *Acta Math.* **52** (1928–9), 92–106．彼以前の幾何学的手法（随伴曲線など）を用いても，すべての楕円曲線が 3 次曲線に双有理同値であることは証明できるが，標準形に帰着できることを示したのは彼が最初である．



すると，曲線 $\mathcal{D}$ は $F(X,Y)=0$，ただし

$$F(X,Y) = F_1(X,Y)+F_2(X,Y)+F_3(X,Y),$$

F_j は次数 j の同次式である．Y–軸は曲線と $(0,y)$ で交わるので

$$0 = yF_1(0,1)+y^2F_2(0,1)+y^3F_3(0,1)$$

である．Y–軸は接線でもあるので，この y に関する 2 次方程式は重根をもつ．つまり，

$$F_2(0,1)^2-4F_1(0,1)F_3(0,1) = 0. \qquad (*)$$

ここで $Y=tX$ と曲線の交点を考えると，

$$0 = xF_1(1,t)+x^2F_2(1,t)+x^3F_3(1,t)$$

を得る．$x=0$ という解を除けば

$$s^2 = F_2(1,t)^2-4F_1(1,t)F_3(1,t)$$

（この右辺を $G(t)$ とおく），ただし

$$s = 2F_3(1,t)x+F_2(1,t)$$

である．ここで $G(t)$ は（$*$）から 3 次式であり，s, t に関する線型変換を用いて標準形を得る．

(iii)　**曲線 $\mathcal{D}$ が $Y^2=$“X の 4 次式” で与えられ，かつ有理点をもつとき**

有理点を (a,b) とおく．座標変換

$$X \to \frac{1}{X-a}, \quad Y \to \frac{Y}{(X-a)^2}$$

を用いて，有理点は無限遠にあるとしてよい．このとき

$$Y^2 = f_0 + f_1 X + f_2 X^2 + f_3 X^3 + f_4 X^4,$$

f_4 は平方数となる．両辺を f_4 で割り，一般性を失うことなく

$$f_4 = 1$$

としてよい．

右辺は

$$G(X)^2 + H(X)$$

という形に書ける．ここで

$$G(X) = X^2 + g_1 X + g_0,$$
$$H(X) = h_1 X + h_0$$

で g_j, h_j は f_j から容易に決まる数である．

このとき曲線の方程式は

$$(Y + G(X))(Y - G(X)) = H(X)$$

と書ける．

$$Y + G(X) = T$$

とおくと，

$$Y - G(X) = \frac{H(X)}{T}$$

および

$$2G(X) = T - \frac{H(X)}{T}$$

である．両辺に T^2 をかけ，$TX = S$ とおけば，

$$2S^2 + 2g_1 TS + 2g_0 T^2 = T^3 - h_1 S - h_0 T$$

を得る．これからたやすく標準形を得る．

（iv）**共通な有理点をもつ 2 次曲面 2 つの交わり**

X, Y, Z, T を同次座標系とし，共通の有理点を $(0,0,0,1)$ とする．このとき 2 次形式は次のように書ける．

$$\left.\begin{aligned} Q_1 &= TL + R \\ Q_2 &= TM + S \end{aligned}\right\}$$

ここで L, M は X, Y, Z に関する 1 次形式，R, S は X, Y, Z に関する 2 次形式である．

まず L と M が 1 次従属と仮定すると，一般性を失うことなく $M=0$ としてよい．すると交わりは

$$S(X,Y,Z)=0, \quad T=R(X,Y,Z)/L(X,Y,Z)$$

であるが，これは種数 0 である．

L と M が 1 次独立であれば，T を消去して

$$C(X,Y,Z)=LS-RM=0,$$

C は同次 3 次式である．これは有理点

$$L(X,Y,Z)=M(X,Y,Z)=0$$

をもつ．これで前出の場合に帰着できた．

【演習問題】

1　次の曲線を標準形に変形せよ．

（i）$X^3+Y^3+dZ^3=0$

（ii）$X^3+Y^3+Z^3-3mXYZ=0$

（iii）$Y^2-kT^2=X^2, \quad Y^2+kT^2=Z^2$

（iv）$X_1^2X_2-X_1X_2^2-X_1X_3^2+X_2^2X_3=0$

2　［難しい］2 次曲面

$$X^2=Y^2-T^2, \quad Z^2=Y^2+T^2$$

の交わりに点 $(1,1,1,0)$ を単位元として群の演算を定義し，$\boldsymbol{x}_3=\boldsymbol{x}_1+\boldsymbol{x}_2$ とおけば

$$\begin{aligned}
x_3 &= x_2t_2y_1z_1-x_1t_1y_2z_2\\
y_3 &= y_2t_2z_1x_1-y_1t_1z_2x_2\\
z_3 &= z_2t_2x_1y_1-z_1t_1x_2y_2\\
t_3 &= t_2^2x_1^2-t_1^2x_2^2=t_2^2y_1^2-t_1^2y_2^2=t_2^2z_1^2-t_1^2z_2^2
\end{aligned}$$

であることを示せ．

3

（i）　次の各曲線について 5 つの元からなる体 $\boldsymbol{F}_5$ 上定義される点をすべて求めよ．

$$Y^2Z = X^3+XZ^2$$
$$Y^2Z = X^3+2XZ^2$$
$$Y^2Z = X^3+Z^3.$$

さらに各曲線について，$\boldsymbol{F}_5$ 上定義された点が $(0,1,0)$ を単位元として与えられる群演算で群になることを確かめよ．

(ii)　他の $\boldsymbol{F}_p$ および曲線

$$Y^2Z = X^3+AXZ^2+BZ^3$$

について前問と同じことを行ない，群が巡回群でないものを見つけよ．また生成元の数が2つより多くなる例は見つかるか？

4　以下に考える曲線では無限遠点が群の単位元となっているものとする．

(i)　楕円曲線 $Y^2=(X-\alpha)(X^2+aX+b)$ について，変換 $\boldsymbol{x}\to\boldsymbol{x}+(\alpha,0)$ は1次分数変換

$$T:\ x \to (t_{11}x+t_{12})/(t_{21}x+t_{22})$$

を引き起こすことを示せ．また T^2: $x\to x$ となることを確かめよ．

(ii)　楕円曲線 $Y^2=(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ について，T_1,T_2,T_3 は(i)で $\alpha=\alpha_j$ $(j=1,2,3)$ とおいて得られる1次分数変換とすれば，T_1,T_2,T_3 は可換であり，

$$T_1T_2T_3:\ x\to x$$

であることを示せ．

(iii)　(i)で $\alpha=\alpha_j$ $(j=1,2,3)$ としたときに対応する 2×2 行列 $\begin{pmatrix} t_{11} & t_{21} \\ t_{12} & t_{22} \end{pmatrix}$ を $\mathcal{T}_j$ とするとき，

$$\mathcal{T}_1\mathcal{T}_2+\mathcal{T}_2\mathcal{T}_1 = 0$$

を示せ．

(iv)　T_1 の不動点を見つけ，それらが T_2 により互いにいれかわることを示せ．

5　直線 $Y=lX+m$ が曲線

$$Y^2 = X^3+AX+B$$

の変曲点における接線となる必要十分条件を求めよ．これから位数3の有理点をもつ曲線の標準形の一般形を求めよ．

6　直線 $Y=lX+m$ が曲線

$$Y^2 = X(X^2+aX+b)$$

の変曲点における接線となる必要十分条件を求めよ．これから位数6の有理点をもつ曲線の標準形の一般形を求めよ．

7 $$F(X,Y,Z)=X^2Y+XZ^2+2Y^3+Z^3$$

とおく．曲線 $F=0$ を標準形に変換する $\boldsymbol{Q}$ 上の双有理変換で，点 $(1,0,0)$ を無限遠点にうつすものを求めよ．

8 2次曲面

$$X_1^2-2X_2^2+X_3^2=0, \quad X_2^2-2X_3^2+X_4^2=0$$

の交わりを標準形にうつす $\boldsymbol{Q}$ 上の双有理変換で，$(1,1,1,1)$ を無限遠点にうつすものを求めよ．

9 前2つの問題と類似の問題を自分で作りそれを解け．

9

退化した曲線の群構造

この章では，曲線

$$\mathcal{C}:\ Y^2 = X^3 + AX + B \tag{1}$$

の係数 A, B が

$$4A^3 + 27B^2 = 0 \tag{2}$$

をみたすときを考える．(2)が成り立たないときは曲線上の群演算は $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ が直線と $\mathcal{C}$ との交点とすれば

$$\boldsymbol{a} + \boldsymbol{b} + \boldsymbol{c} = 0$$

であったことを思い出そう[*1]．非特異点上ではこれがそのままの退化した(2)の場合にも群構造を与えることを示そう．

2 通りの場合があり，第 2 の場合はさらに 2 通りに分れる．

第 1 の場合（尖点（cusp））　$A = B = 0$ としよう．すると

$$\mathcal{C}:\ Y^2Z = X^3$$

であり，原点が特異点となる．原点を通らない直線は

$$Z = lX + mY$$

と書け，この直線は

$$X^3 - Y^2(lX + mY) = 0$$

をみたす点で交わる．3 つの交点を (x_j, y_j, z_j) $(j = 1, 2, 3)$ とすれば

*1　単位元については 0 と $\boldsymbol{o}$ は区別せずに用いる．

$$u_1 + u_2 + u_3 = 0$$

である．ただし，

$$u_j = x_j / y_j$$

である．

したがって，無限遠点 $(0,1,0)$ を単位元とするような加法群を得る．

第 2 の場合[*2] **(通常 2 重点**(標数 $\neq 2$)) A, B 共に 0 でなければ，$X \to X+$(定数) という変数変換を行なって

$$\mathcal{C}: \ Y^2 Z = X^2(X + CZ) \qquad (C \neq 0),$$

すなわち，

$$(Y^2 - CX^2)Z = X^3$$

を得る．C が $C = \gamma^2$ という平方数のときは

$$U = Y + \gamma X, \quad V = Y - \gamma X$$

とおけば，$\mathcal{C}$ は

$$8\gamma^3 UVZ = (U - V)^3$$

で与えられる．

原点を通らない直線は

$$Z = lU + mV$$

と書け，$\mathcal{C}$ とは

$$(U - V)^3 - 8\gamma^3 UV(lU + mV) = 0$$

をみたす点で交わる．交点を (u_j, v_j, z_j) $(j = 1, 2, 3)$ とおけば

$$\left(\frac{u_1}{v_1}\right)\left(\frac{u_2}{v_2}\right)\left(\frac{u_3}{v_3}\right) = 1$$

となり，乗法群を得る．

C が平方数でないときは，$\gamma^2 = C$ をみたす γ を基礎体につけ加える．$\mathcal{C}$ 上の点 (x, y, z) に対し，例えば

$$\frac{y + \gamma x}{y - \gamma x} = r + s\gamma \qquad (*)$$

---

*2　この場合の詳細な部分はあとで不必要である．

（ただし，$r^2-s^2C=1$ である）とおく．こうして（$*$）上の "ねじれた" 乗法を得る．これを $x^2+y^2=1$ をみたす複素数 $x+iy$ の乗法になぞらえてみよ． □

進んだ読者向けの注意　標数 2 のときは

$$\mathcal{C}:\ Y^2Z = X^3+AXZ^2+BZ^3$$

は常に特異である．方程式を

$$(Y^2-BZ^2)Z = X(X^2+AZ^2)$$

と書けば，有限体（より一般に完全体）上では

$$B=\beta^2,\quad A=\alpha^2$$

をみたす α, β が存在するから，曲線は

$$(Y+\beta Z)^2Z = X(X+\alpha Z)^2$$

となるが，これは明らかに特異である．

基礎体が完全体でないときは，純非分離拡大体上定義される特異点の例がありうる．第 6 章の最初の脚注を参照のこと．

10

還　　元

この章の背後にある考え方は，局所体 $\boldsymbol{Q}_p$ を通して有理数体 $\boldsymbol{Q}$ 上の問題を考えるのと同様に，有限体 $\boldsymbol{F}_p$ への p を法とする還元を通して $\boldsymbol{Q}_p$ 上の問題を考えようということである．ここでは応用上必要になる範囲のみを述べることにする．

p を法とする還元の写像 $\boldsymbol{Z}_p \to \boldsymbol{F}_p$ をバー $a \to \overline{a}$ で表す．これは以下のようにして対応する射影平面 $V, \overline{V}$ に拡張される．V の点 $\boldsymbol{a}$ の射影座標を (a_1, a_2, a_3) とおく．a_1, a_2, a_3 に $\boldsymbol{Q}_p$ の同じ元をかけて一般性を失うことなく

$$\max\{|a_1|, |a_2|, |a_3|\} = 1$$

としてよい．ただし，$|\ \ | = |\ \ |_p$ である．すると $(\overline{a}_1, \overline{a}_2, \overline{a}_3)$ は $\overline{V}$ の点 $\overline{\boldsymbol{a}}$ の座標として意味をもつ．

同様にして，直線

$$\boldsymbol{l}: \ l_1X_1 + l_2X_2 + l_3X_3 = 0$$

の還元 $\overline{\boldsymbol{l}}$ が定義できる．点 $\boldsymbol{a}$ が直線 $\boldsymbol{l}$ 上にあれば明らかに点 $\overline{\boldsymbol{a}}$ は $\overline{\boldsymbol{l}}$ 上にある．

$\boldsymbol{Q}_p$ 上定義された 3 次曲線

$$\mathcal{C}: \ F(\boldsymbol{X}) = 0$$

の還元にはいろいろな方法があるが，ここではもっとも単純なものを考えれば十分である．$F(\boldsymbol{X})$ はすべては 0 でない $f_{ijk} \in \boldsymbol{Q}_p$ を用いて

$$F(\boldsymbol{X}) = \sum_{i \leqq j \leqq k} f_{ijk} X_i X_j X_k \in \boldsymbol{Q}_p[\boldsymbol{X}]$$

と書くことができ，しかも一般性を失うことなく

$$\max_{i,j,k} |f_{ijk}| = 1$$

と仮定してよい．すると

$$\overline{F}(\boldsymbol{X}) = \sum_{i \leqq j \leqq k} \overline{f}_{ijk} X_i X_j X_k \in \boldsymbol{F}_p[\boldsymbol{X}]$$

は多項式として 0 ではなく，$\boldsymbol{F}_p$ 上の曲線

$$\overline{\mathcal{C}} : \ \overline{F}(\boldsymbol{X}) = 0$$

を定める．もちろん，この曲線が可約[*1]ということもある．

$\boldsymbol{a}$ が $\mathcal{C}$ 上の点ならば，$\overline{\boldsymbol{a}}$ は明らかに $\overline{\mathcal{C}}$ 上の点である．少し弱い主張であるけれどもこの逆が成立する．

補題 1　$\overline{\mathcal{C}}$ 上の非特異な点 $\overline{\boldsymbol{b}}$ に対して，$\overline{\boldsymbol{a}} = \overline{\boldsymbol{b}}$ をみたす $\mathcal{C}$ 上の点 $\boldsymbol{a}$ が存在する． □

注意　$\overline{\boldsymbol{b}}$ という表現は $\boldsymbol{F}_p$ 上定義された点を意味し，点 $\boldsymbol{b}$ の還元として得られることを意味しているわけではない．$\overline{\boldsymbol{b}}$ が点 $\boldsymbol{a}$ の還元として得られるとき，$\overline{\boldsymbol{b}}$ は $\boldsymbol{a}$ に“持ち上がる”という．例えば，$\overline{\mathcal{C}}$ 上の特異点が $\mathcal{C}$ 上の点に持ち上がることもあるし，そうでないこともあることは容易にわかる（演習問題参照）．

ニュートンによる逐次近似法で $\boldsymbol{a}$ を構成しよう．p–進解析では一般的に Hensel の補題とよばれているものである．

補題 2　$\boldsymbol{Z}_p[T]$ の元 $G(T)$ と，$\boldsymbol{Z}_p$ の元 t_0 が

$$|G(t_0)| < 1, \quad |G'(t_0)| = 1$$

をみたすものとする．ただし G' は G の形式的な微分を表すものとする．すると

$$G(t) = 0, \quad |t - t_0| \leqq G(t_0)$$

をみたす $\boldsymbol{Z}_p$ の元 t が存在する． □

上記の Hensel の補題を少しの間仮定しておいて，補題 1 を証明しよう．$\overline{\boldsymbol{b}}$ は $\overline{\mathcal{C}}$ 上の非特異な点だから，

---

*1　$\overline{F}(\boldsymbol{X})$ が分解することを意味する．

$$\frac{\partial \overline{F}}{\partial X_1}(\bar{\boldsymbol{b}}) \neq 0$$

と仮定してよい．$\boldsymbol{Z}_p$ の元 b_j を $\bar{\boldsymbol{b}}=(\bar{b}_1, \cdots, \bar{b}_n)$ をみたすようにとる．

するとHenselの補題の仮定が

$$G(T) = F(T, b_2, \cdots, b_n), \quad t_0 = b_1$$

について成立する．$\boldsymbol{a}=(t, b_2, \cdots, b_n)$ とおく．ここで t はHenselの補題から得られるものである．明らかに $F(\boldsymbol{a})=0$, $\bar{\boldsymbol{a}}=\bar{\boldsymbol{b}}$ であり，$\boldsymbol{a}$ が求めるべきものである．

残るはHenselの補題の証明である．U を不定元とする．すると

$$G(T+U) = G(T)+UG_1(T)+U^2G_2(T)+\cdots$$

である．ただし，$G_j \in \boldsymbol{Z}_p[T]$, $G_1=G'$ である．ここで

$$u = -G(t_0)/G'(t_0)$$

とおけば

$$G(t_0+u) = u^2G_2(t_0)+u^3G_3(t_0)+\cdots$$

であるから

$$|G(t_1)| \leqq |G(t_0)|^2$$

である．ここで

$$t_1 = t_0+u$$

とおいた．明らかに

$$|G'(t_1)| = |G'(t_0)| = 1\,.$$

この手続きを繰り返して基本列 t_j $(t \geqq 0)$ を得る．t_j の極限値 t が求めるものにほかならない．

さて，還元の後，直線と3次曲線の交わりがどうなるかということも考える必要がある．すでにみたように，$\boldsymbol{l}$ が $\mathcal{C}$ と $\boldsymbol{a}$ で交わるとき，$\overline{\boldsymbol{l}}$ と $\overline{\mathcal{C}}$ は $\overline{\boldsymbol{a}}$ で交わる．ところで，$\boldsymbol{l}$ が $\mathcal{C}$ と相異なる点 $\boldsymbol{a}, \boldsymbol{b}$ と交わり，$\overline{\boldsymbol{a}}=\overline{\boldsymbol{b}}$ となるときその交点で重複度が2以上であるといえるだろうか？

次の補題はこのことが正しいことを保証している．

補題3　直線 $\boldsymbol{l}$ が3次曲線 $\mathcal{C}$ と $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ で交わっているとする．ただし重複点はその重複度だけ与えられているとする（例えば，$\boldsymbol{a}$ で2重に交わって

いるときは$\boldsymbol{b}=\boldsymbol{a}$である）．このとき

（I） $\bar{\boldsymbol{l}}$は$\overline{C}$に含まれるか，または

（II） $\bar{\boldsymbol{l}}$は$\overline{C}$と$\bar{\boldsymbol{a}}$, $\bar{\boldsymbol{b}}$, $\bar{\boldsymbol{c}}$で交わる．ただし，重複点では重複度だけ同じ点が与えられているとする．

［証明］ 一般性を失うことなく

$$|l_3| = 1 = \max(|l_1|, |l_2|, |l_3|)$$

としてよい．

$$G(X_1, X_2) = F(X_1, X_2, -l_1X_1 - l_2X_2) \\ \in \boldsymbol{Z}_p[X_1, X_2]$$

とおけば，その還元は

$$\overline{G}(X_1, X_2) = \overline{F}(X_1, X_2, -\bar{l}_1X_1 - \bar{l}_2X_2)$$

である（訳者注．$X_3 = -\dfrac{l_1}{l_3}X_1 - \dfrac{l_2}{l_3}X_2$で$|l_3| = 1$なので，上記のように$G(X_1, X_2)$を定義して還元してもよい）．

$\overline{G}(X_1, X_2) = 0$ならば(I)の場合である．したがって

$$\overline{G}(X_1, X_2) \neq 0$$

と仮定しよう．$\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$の成分を

$$\max(|a_1|, |a_2|, |a_3|) = 1$$

など，となるように標準化しておくと，$\boldsymbol{a}$は$\boldsymbol{l}$上にあるから

$$(\bar{a}_1, \bar{a}_2) \neq (0, 0)$$

など，が従う．仮定から

$$G(X_1, X_2) = \lambda(a_2X_1 - a_1X_2)(b_2X_1 - b_1X_2)(c_2X_1 - c_1X_2) \\ = \lambda H(X_1, X_2)$$

をみたす$\boldsymbol{Q}_p$の元λが存在する．ここで

$$\overline{H}(X_1, X_2) = (\bar{a}_2X_1 - \bar{a}_1X_2)(\bar{b}_2X_1 - \bar{b}_1X_2)(\bar{c}_2X_1 - \bar{c}_1X_2) \\ \neq 0.$$

$\overline{G}$と$\overline{H}$は定数倍しか違わず，これで補題が証明された． ∎

【演習問題】

1

（i）　$\boldsymbol{Q}_p$ 上の曲線 $\mathcal{C}$: $Y^2=X^3+p$ に対して，p を法として還元して得られる曲線上の点 $(0,0)$ は $\mathcal{C}$ 上の点に持ち上がらないことを示せ．

（ii）　$\boldsymbol{Q}_p$ 上の楕円曲線 $\mathcal{C}$ で p を法として還元して得られる曲線が尖点をもつような例を与えよ．

2　$\boldsymbol{Q}_p$ 上の曲線 $\mathcal{C}$ で p を法として還元して得られる曲線が，

（i）$\mathcal{C}$ の上に持ち上がるような通常 2 重点をもつもの，

（ii）$\mathcal{C}$ の上に持ち上がらないような通常 2 重点をもつようなものをそれぞれ構成せよ．

11

p–進体上の楕円曲線

$\boldsymbol{Q}_p$ 上の楕円曲線

$$\mathcal{C}:\ Y^2 = X^3 + AX + B$$

を考える．したがって

$$4A^3 + 27B^2 \neq 0$$

であり，一般性を失うことなく

$$A,\ B \in \boldsymbol{Z}_p$$

と仮定してよい．この章では $\boldsymbol{Q}_p$ 上定義される $\mathcal{C}$ の点のなす群 $\mathfrak{G}$ について考察する．

この章では前章で述べた還元の理論を用いる．このため，$\mathcal{C}$ を同次座標を用いて

$$\mathcal{C}:\ Y^2Z = X^3 + AXZ^2 + BZ^3$$

と書く．$\boldsymbol{F}_p$ 上の曲線

$$\overline{\mathcal{C}}:\ Y^2Z = X^3 + \overline{A}XZ^2 + \overline{B}Z^3$$

は第 10 章の補題 3 によれば特異かもしれないが，$\overline{\mathcal{C}}$ は直線は含まない．

$\overline{\mathfrak{G}}$ は $\overline{\mathcal{C}}$ の $\boldsymbol{F}_p$ 上定義された点全体を表す．$\overline{\mathfrak{G}}^{(0)}$ は $\overline{\mathfrak{G}}$ の部分集合で非特異な点全体からなるものとする．$\mathfrak{G}^{(0)} \subset \mathfrak{G}$ は p を法とする還元が $\overline{\mathfrak{G}}^{(0)}$ に入る点からなる $\mathfrak{G}$ の部分集合とする．第 10 章の補題 1 から写像

$$\mathfrak{G}^{(0)} \to \overline{\mathfrak{G}}^{(0)}$$

は全射である．

群構造はどうなるであろうか？　$\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathfrak{G}$ が

$$\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}=\boldsymbol{o}$$

をみたすとする．この関係は $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ が $\mathcal{C}$ と直線 $\boldsymbol{l}$ の交点であるとき，またそのときに限り成り立つ．すると，$\overline{\boldsymbol{a}}, \overline{\boldsymbol{b}}, \overline{\boldsymbol{c}}$ は $\overline{\mathcal{C}}$ と $\overline{\boldsymbol{l}}$ との交点である．$\overline{\mathcal{C}}$ 上では非特異な点についてのみ群演算を定義したので，$\overline{\boldsymbol{a}}, \overline{\boldsymbol{b}}, \overline{\boldsymbol{c}} \in \overline{\mathfrak{G}}^{(0)}$ ならば，

$$\overline{\boldsymbol{a}}+\overline{\boldsymbol{b}}+\overline{\boldsymbol{c}}=\overline{\boldsymbol{o}}$$

が成立する．

以上をまとめれば，$\overline{\mathfrak{G}}^{(0)}$ への全射準同型があるような $\mathfrak{G}$ の部分群 $\mathfrak{G}^{(0)}$ が得られることがわかる．準同型 $\mathfrak{G}^{(0)} \to \overline{\mathfrak{G}}^{(0)}$ の核は $\overline{\boldsymbol{o}}$ へうつされる点全体，すなわち，非同次な座標を用いれば $\boldsymbol{o}$ と $x \notin \boldsymbol{Z}_p$ かつ $y \notin \boldsymbol{Z}_p$ をみたす $\mathfrak{G}$ の点 (x, y) である．これは**還元の核**とよばれる．

次に還元の核の構造についてみていこう．$(x, y) \in \mathfrak{G}$ で $x, y \notin \boldsymbol{Z}_p$ ならば $|y|^2=|x|^3$ であるから

$$|x|=p^{2n}, \quad |y|=p^{3n}$$

をみたすような $n \geqq 1$ が存在する．この n を (x, y) のレベルとよぶ．定義から，(x, y) が還元の核に入ってなければレベルは 0 である．$\boldsymbol{o}$ のレベルは ∞ と約束する．

さて，整数 $N \geqq 1$ に対し座標変換

$$X_N=p^{2N}X, \quad Y_N=p^{3N}Y, \quad Z_N=Z$$

を考えれば，$\mathcal{C}$ の方程式は

$$\mathcal{C}_N: \ Y_N^2 Z_N=X_N^3+p^{4N}AX_N Z_N^2+p^{6N}BZ_N^3$$

となる．p を法とする還元に関しこの新しい座標を使えば，得られる曲線は

$$\overline{\mathcal{C}}_N: \ Y_N^2 Z_N=X_N^3$$

である．

前に行なったことをこの新たな状況で考えてみよう．点 (x, y) のレベル $<N$ ならば $\overline{\mathcal{C}}_N$ の特異点 $(0,0)$ にうつされ，レベル $>N$ ならば還元の核に含まれる．そして，$\boldsymbol{F}_p$ 上定義された $\overline{\mathcal{C}}_N$ の非特異点のなす群は $\boldsymbol{F}_p$ の加法群である．前と同様それは $\mathfrak{G}$ の像に含まれる．

$N \geqq 1$ に対し $\mathfrak{G}^{(N)}$ を $\mathfrak{G}$ のレベル $\geqq N$ の点からなる部分集合とおけば，次

の補題が得られたわけである．

補題 1　部分群の列

$$\mathfrak{G} \supset \mathfrak{G}^{(0)} \supset \mathfrak{G}^{(1)} \supset \cdots \supset \mathfrak{G}^{(N)} \supset \cdots$$

において，$N \geqq 1$ のとき商群 $\mathfrak{G}^{(N)}/\mathfrak{G}^{(N+1)}$ は位数 p の巡回群である．商群 $\mathfrak{G}^{(0)}/\mathfrak{G}^{(1)}$ は $\overline{C}$ の非特異点がなす群に同型となる．さらに

$$\bigcap_N \mathfrak{G}^{(N)} = \{\boldsymbol{o}\}$$

である．□

この群の列はp–**進フィルトレーション**とよばれる．

系　$\boldsymbol{x}=(x,y)\in\mathfrak{G}$ は位数が p と互いに素な有限位数の元とする．このとき，$x, y \in \boldsymbol{Z}_p$ である．

［証明］　$\boldsymbol{x}$ のレベルが $n \geqq 1$ ならば，$\boldsymbol{x}\in\mathfrak{G}^{(n)}$ かつ $\boldsymbol{x}\notin\mathfrak{G}^{(n+1)}$ で $\mathfrak{G}^{(n)}/\mathfrak{G}^{(n+1)}$ の 0 でない元にうつされるが，この像の位数は p である．∎

次の目標は上の系の“位数が p と互いに素”という仮定を取り除くことにある．

$\mathfrak{G}^{(N)}/\mathfrak{G}^{(N+1)}$ から加法群への準同型は

$$(x,y) \to p^{-N}x/y \quad \mathrm{mod}\, p$$

で与えられる．

$\boldsymbol{x}\in\mathfrak{G}^{(1)}$ に対し関数 $u(\boldsymbol{x})$ を次のように定義する．

$$u(\boldsymbol{x}) = x/y \qquad (\boldsymbol{x}=(x,y)),$$
$$u(\boldsymbol{o}) = 0.$$

$\boldsymbol{x}$ のレベルが n ならば，$|u(\boldsymbol{x})|=p^{-n}$ となることに注意しよう．

補題 2　$\boldsymbol{x}_1, \boldsymbol{x}_2\in\mathfrak{G}^{(1)}$ であれば，

$$|u(\boldsymbol{x}_1+\boldsymbol{x}_2)-u(\boldsymbol{x}_1)-u(\boldsymbol{x}_2)| \leqq \max\{|u(\boldsymbol{x}_1)|^5, |u(\boldsymbol{x}_2)|^5\}$$

が成り立つ．

［証明］　$\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_1+\boldsymbol{x}_2$ の中に $\boldsymbol{o}$ は含まれてないと仮定してよく，さらに一般性を失うことなく

$$|u(\boldsymbol{x}_1)| \geqq |u(\boldsymbol{x}_2)|$$

としてよい．$\boldsymbol{x}_1$ のレベルを N とし，先に導入した座標 X_N, Y_N，および曲

線 $\mathcal{C}_N$ を用いる．

$\boldsymbol{x}_1$ も $\boldsymbol{x}_2$ も $\overline{\mathcal{C}}_N$ の特異点 $(0,0)$ にはうつされないので，この 2 点を結ぶ直線は

$$Z_N = lX_N + mY_N$$

ただし

$$|l| \leqq 1, \quad |m| \leqq 1$$

という形に書ける．この直線は以下の方程式をみたす点で $\mathcal{C}_N$ と交わる．

$$0 = -Y_N^2(lX_N+mY_N)+X_N^3+p^{4N}AX_N(lX_N+mY_N)^2$$
$$+p^{6N}B(lX_N+mY_N)^3$$

この右辺を

$$c_3X_N^3+c_2X_N^2Y_N+c_1X_NY_N^2+c_0Y_N^3 \qquad (*)$$

とおく．ここで

$$c_3 = 1+p^{4N}Al^2+p^{6N}Bl^3$$
$$c_2 = 2p^{4N}lmA+3p^{6N}l^2mB$$

である．したがって

$$|c_3| = 1, \quad |c_2| \leqq p^{-4N}$$

である．

$(*)$の解 X_N/Y_N は $-p^{-N}u(\boldsymbol{x}_1+\boldsymbol{x}_2)$，$p^{-N}u(\boldsymbol{x}_1)$ および $p^{-N}u(\boldsymbol{x}_2)$ である．これらの解の和は $-c_2/c_3$ であるから，結果が従う． ▌

系 1　$\boldsymbol{x}\in\mathfrak{G}^{(1)}$, $s\in\boldsymbol{Z}$ ならば

$$|u(s\boldsymbol{x})| = |s||u(\boldsymbol{x})|.$$

［証明］　帰納法を用いて，$s>0$ ならば

$$|u(s\boldsymbol{x})-su(\boldsymbol{x})| \leqq |u(\boldsymbol{x})|^5$$

であるから，$p\nmid s$ または $s=p$ のときは結果を得る．あとは s の p ベキに関する帰納法を用いればよい． ▌

系 2　$\mathfrak{G}^{(1)}$ は 有限位数の元をもたない．

系 3　$p\neq 2$ かつ $|4A^3+27B^2|=1$ とする．$\mathfrak{G}$ の有限位数の元全体からなる部分群は $\overline{\mathfrak{G}}$ の部分群に同型である．

［証明］　$\mathfrak{G}=\mathfrak{G}^{(0)}$ かつ

$$\overline{\mathfrak{G}}=\mathfrak{G}/\mathfrak{G}^{(1)}$$

で $\mathfrak{G}^{(1)}$ は有限位数の元をもたないから．∎

進んだ読者向けの注意　この章で行なったことはすべて $\boldsymbol{Q}_p$ の代数拡大体の場合に一般化できる．位数が p と素な有限位数の元が整数の座標をもつことはそのまま成立するが，位数が p ベキのものについては，そこで拡大が分岐するときには成立しないことがある．

十分大きな N に関して群 $\mathfrak{G}^{(N)}$ のパラメーター表示を与える $u=u(x)$ のベキ級数が存在する．これはもともと複素変数での公式から得られるものである．形式群(formal group)や 形式的対数関数(formal logarithm)を用いた現代的な手法については，例えば巻末に紹介してある Silverman の本を参照のこと．

12

有限位数の元

$\boldsymbol{Q}$ 上の楕円曲線

$$\mathcal{C}:\ Y^2 = X^3 + AX + B$$

を考える．したがって

$$4A^3 + 27B^2 \neq 0$$

である．ここで

$$A,\ B \in \boldsymbol{Z}$$

としてよい．

定理 1　$\mathcal{C}$ の有限位数の有理点のなす群は有限群である．$(x, y) \neq \boldsymbol{o}$ の位数が有限ならば

$$x, y \in \boldsymbol{Z}$$

であり，

$$y = 0 \quad \text{または} \quad y^2 \mid (4A^3 + 27B^2)$$

である．

［証明］ $\mathcal{C}$ の $\boldsymbol{Q}$ 上定義された点のなす群を $\mathfrak{G}$ とし，$\boldsymbol{Q}_p$ 上定義された点のなす群を $\mathfrak{G}_p$ とする．ここで p は素数である．

$(x, y) \neq (0, 0)$ の位数は有限とする．すると $\mathfrak{G} \subset \mathfrak{G}_p$ であるから，

$$x \in \boldsymbol{Z}_p, \quad y \in \boldsymbol{Z}_p$$

が任意の p について成り立つ．ゆえに

$$x \in \boldsymbol{Z}, \quad y \in \boldsymbol{Z}$$

である．

さて，p は $p\neq 2$，$p\nmid(4A^3+27B^2)$ をみたす任意の素数とする．すると，前章の最後の系 3 から $\mathfrak{G}$ のねじれ部分群は $\boldsymbol{F}_p$ 上定義される点のなす群の部分群に同型である．したがって，ねじれ部分群の位数は有限である．いろいろな p を用いて，一般にねじれ部分群の位数を厳密に調べることもできるが，以下の方法を使えば，位数有限の元そのものを容易に見つけることができる．

$2(x,y)=\boldsymbol{o}$ ならば，$y=0$ である．もし (x,y) の位数が 2 でなければ，$2(x,y)=(x_2,y_2)$ とおけば (x_2,y_2) はまた位数有限であるから，x_2, $y_2\in\boldsymbol{Z}$ である．

(x,y) における接線を考えれば，

$$x_2+2x=\left(\frac{3x^2+A}{2y}\right)^2=\frac{(3x^2+A)^2}{4(x^3+Ax+B)}$$

を得る（公式集参照）．ゆえに $y^2=x^3+Ax+B$ は $(3x^2+A)^2$ を割り切る．

ところが，容易にわかるように，$\boldsymbol{Z}[X,A,B]$ において

$$(3X^2+4A)(3X^2+A)^2\equiv 4A^3+27B^2 \mod (X^3+AX+B) \qquad (*)$$

である．こうして

$$y^2\mid(4A^3+27B^2)$$

を得る．［等式(∗)に関して詳しいことは，第 16 章を参照せよ．］ ▮

注意　$AB=0$ のときには $\mathcal{C}$ の位数有限の元に関してもっと強力な結果があるが，それについてはこの章の演習問題をみよ．Mazur は，ねじれ部分群のありうる形をすべて決定した．ねじれ部分群は次のいずれかであり，すべての場合が実際におこる．

$$\boldsymbol{Z}/n\boldsymbol{Z} \qquad 1\leqq n\leqq 10 \quad \text{または} \quad n=12$$

または

$$\boldsymbol{Z}/2\boldsymbol{Z}\times\boldsymbol{Z}/2n\boldsymbol{Z} \qquad 1\leqq n\leqq 4$$

である．

【演習問題】

1　以下の楕円曲線の $\boldsymbol{Q}$ 上のねじれ部分群を求めよ．

（i）　$Y^2=X^3+1$

（ii）　$Y^2=X^3-43X+166$

（iii）　$Y^2=X^3-219X+1654$

（iv）　$Y^2=X(X-1)(X+2)$

（v）　$Y^2=X(X+1)(X+4)$

（vi）　$X^3+Y^3+Z^3-15XYZ=0$

（vii）　$Y^2=X(X+81)(X+256)$

（viii）　$X_1^2X_2-X_1X_2^2-X_1X_3^2+X_2^2X_3=0$

［注意．上記の例は勝手に与えたものではない！］

2　次の定理の証明の概略の行間を埋めよ[*1]［もしくは，よりよい証明を与えよ！］．

定理　4 ベキの因子を含まない整数 A に対し，

$$\mathcal{C}:\ Y^2=X(X^2+A)$$

上の位数有限の点はすべて以下の(I)，(II)，(III)で与えられる．

（I）　位数 2 の点 $(0,0)$，

（II）　$A=4$ ならば点 $(2,\pm 4,1)$ の位数は 4 である．

（III）　$A=-C^2$ である整数 C があれば点 $(\pm C,0)$ の位数は 2 である．

［証明の概略］

（i）　$(x,y)=2(a,b)$ ならば

$$x=(a^2-A)^2/4b^2$$

である．

（ii）　位数 2 の点は上記に述べた通りである．

（iii）　$(0,0)=2(a,b)$ をみたす (a,b) が存在するのは $A=4$ のときに限る．また，$(\pm C,0)=2(a,b)$ をみたす (a,b) は存在しない．

以下 (a,b) の位数は奇数とする．

（iv）　a は平方数である．

（v）　$d=\gcd(a,A)$ とおけば，$a=da_1$，$A=dA_1$，$b=db_1$ である．ただし，$b_1^2=a_1(da_1^2+A_1)$ である．

（vi）　$\gcd(f,g)=1$，$a_1=\pm f^2$，$da_1^2+A_1=\pm g^2$，$b_1=fg$，$d=\pm h^2$ をみたす整数

*1　T. Nagell: Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre. *Skrifter utg. av det norske vidensk.-akad i Oslo, Mat.-naturv. kl.* **1935**, No 1, 1–25 参照．

f, g, h がある.

(vii) $a^2-A=2h^4f^4-h^2g^2$, $b=\pm h^2fg$.

(viii) $a^2-A\equiv 0 \pmod{2b}$.

(ix) したがって $f=1$, $g\equiv 0 \pmod 2$, $h\equiv 0 \pmod 2$.

［ヒント. まず $f|g$ を示す.］

(x) ゆえに $2^4|A$.

(xi) 矛盾！ ∎

3 以下の定理の証明の概略の行間を埋めよ*2［もしくは, よりよい証明を与えよ !］.

定理 6 ベキの因子をもたない整数 B に対して,

$$\mathcal{C}:\ Y^2 = X^3+B$$

のすべての位数有限の点は以下のように与えられる.

(I) $B=C^2$ ならば $(0,\pm C)$ は位数 3 である.

(II) $B=D^3$ ならば $(-D,0)$ は位数 2 である.

(III) $B=1$ ならば $(2,\pm 3)$ は位数 6 である.

(IV) $B=-432=-2^4\cdot 3^3$ ならば $(12,\pm 36)$ は位数 3 である.

［証明の概略］

(i) $(x,y)=2(a,b)$, $b\neq 0$ ならば

$$x = (w-2)a, \quad w = 9a^3/4b^2$$

である.

(ii) 2 ベキの位数をもつ元は上記に述べたもののみである.

(iii) $(0,b)$ の形の元の位数は 3 である.

以下, (a,b) の位数は奇数で $a\neq 0$ とする. 要は $w\in \boldsymbol{Z}$ となることを示すことである. すると, $w=1, 2, 3$ のときは簡単に取り扱え, それ以外のときは $|x|_\infty > |a|_\infty$ であり, 2 倍写像を繰り返せば $|x|_\infty \to \infty$ となって矛盾である. $w\in \boldsymbol{Z}$ となることの概略を示そう.

(iv) $p|B$, $p\nmid a$ ならば $p\nmid x$.

(v) $p|B$, $p\nmid x$ ならば $p\nmid a$.

［ヒント. 2 倍写像を繰り返し用いよ.］

---

*2 この結果は R. Fueter: Ueber kubische diophantische Gleichungen. *Comm. Math. Helv.* **2** (1930), 68–69 によるが, その方法は L. J. Mordell: The infinity of rational solutions of $y^2=x^3+k$. *J. London Math. Soc.* **41** (1966), 523–525 をもとにしている.

(vi)　$3^l \| b$, $3^m \| a$ ならば $l=0,1$, または $l=2$, $m \geqq 1$ である.

［ヒント. $l=3$ ならば $3 \nmid x$ か $3^6 | B$ となることを導け.］

(vii)　したがって $w \in \boldsymbol{Z}_3$.

(viii)　$w \in \boldsymbol{Z}_2$.

(ix)　$q|B$, $q \neq 2,3$ をみたす q に関し $w \in \boldsymbol{Z}_q$.

(x)　ゆえに $w \in \boldsymbol{Z}$. ∎

4　曲線

$$X^3+Y^3+dZ^3=0$$

は曲線

$$Y^2 = X^3 - 2^4 \cdot 3^3 \cdot d^2$$

に双有理同値になることを示せ. 正の整数 d が 3 ベキの因数を含まなければ, 前の問題から位数が有限となる点は以下のものに限ることを示せ.

$$d=1, \quad (1,0,-1)\ (0,1,-1) \qquad \text{位数 } 3$$

$$d=1, \quad (1,1,-1) \qquad \text{位数 } 2$$

第 6 章の例外点に関する結果と比べてみよ.

5　$s \in \boldsymbol{Q}$ とする.

$$X^3+sX+k=0$$

が 3 つの有理数解をもつような有理数 k が 1 つあれば, そのような有理数は無限個存在することを示せ.

［ヒント. u を 1 つの有理数解とする. s, u, k を用いて残りの 2 つが有理数である条件を求めよ.］

6　$k \in \boldsymbol{Q}$, $k \neq 0$ とする. 方程式

$$X^3+sX+k=0$$

が 3 つの有理数解をもつような有理数 s が 2 つあれば, そのような有理数は無限個存在することを示せ.

13

有限生成定理(証明の方針)

これからあとの数章の目標は，次の定理を証明することである．

定理 1 $\boldsymbol{Q}$ 上定義された楕円曲線の有理点のなす可換群 $\mathfrak{G}$ は有限生成である． □

この定理は最初 Mordell によって証明され，Weil が代数体上のものに一般化した．普通，**Mordell**(または **Mordell–Weil**)**の有限生成定理**とよばれる．

例えば[*1]，C が

$$Y^2 = X(X^2+877)$$

のときは群 $\mathfrak{G}$ は位数 2 の元 $(0,0)$ と位数無限大の元 $(u/v, r/s)$ で生成される．ここで

$$\begin{aligned}
u &= 37\,5494\,5281\,2716\,2193\,1055\,0406\,9942\,0927\,9234\,6201,\\
v &= 6215\,9877\,7687\,1505\,4254\,6322\,0780\,6972\,3804\,4100,\\
r &= 256\,2562\,6798\,8926\,8093\,8877\,6834\,0455\,1308\,9648\,6691\,5320\\
&\quad 4356\,6034\,6478\,6949,\\
s &= 4900\,7802\,3219\,7875\,8895\,9802\,9339\,9592\,8925\,0960\,6161\,6470\\
&\quad 7799\,7926\,1000
\end{aligned}$$

である．

*1 A. Bremner, J.W.S. Cassels: On the equation $Y^2 = X(X^2+p)$. *Math. Comp.* **42** (1984), 257–264.

定理1の証明はそれぞれ異なったアイデアとテクニックを要する2つの部分に分かれる.

（i） "弱有限生成定理"（または弱い意味の Mordell–Weil の定理），すなわち

$$\mathfrak{G}/2\mathfrak{G}$$

が有限であるという定理．証明は $\mathfrak{G}/2\mathfrak{G}$ から有限群への写像を構成することによりなされる．$\mathfrak{G}$ が位数2の元をもつときは比較的証明がやさしいのでまずこの場合を証明する．そのため，まず同種写像(isogeny)について学ぶ.

弱有限生成定理の証明が構成的でないのは注目すべきことであろう──つまり $\mathfrak{G}/2\mathfrak{G}$ を求めるのに有効な方法を与えてはいない．また，そのアルゴリズムは現在においても知られていない.

（ii） 有限生成定理の2つめの部分は "降下法(descent)" である．$\mathfrak{G}/2\mathfrak{G}$ の代表系 $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_r$ が得られたとしよう．そして $\boldsymbol{a}$ を任意の有理点とする．すると，

$$\boldsymbol{a}-\boldsymbol{b}_s \in 2\mathfrak{G}$$

をみたす s $(1 \leqq s \leqq r)$ が存在する．つまり，この s に対し

$$\boldsymbol{a} = \boldsymbol{b}_s + 2\boldsymbol{c}, \quad \boldsymbol{c} \in \mathfrak{G} \qquad (*)$$

をみたす $\boldsymbol{c}$ が存在する.

高さ(height)は $\mathfrak{G}$ の点の座標の値の大きさを計る関数である．例えば，$\boldsymbol{x} = (x, y)$, $x = u/v$ で u, v は互いに素な整数とすれば，$H(\boldsymbol{x}) = \max(|u|, |v|)$（絶対値）である． この高さに対し $H(\boldsymbol{a}) > H_0$ ならば，（$*$）から $H(\boldsymbol{c}) < H(\boldsymbol{a})$ となるような H_0 が存在することを証明する．これから，$\mathfrak{G}$ は $\boldsymbol{b}_s$ たちと $H(\boldsymbol{a}) \leqq H_0$ をみたす有限個の $\boldsymbol{a}$ から生成されることがわかる.

Fermat による降下法を解説してこの章を終えよう.

Fermat は，方程式

$$X^4 + Y^4 = Z^4 \qquad X \neq 0,\ Y \neq 0$$

が整数解をもたないことを証明しようとした．この曲線は種数3の曲線(Fermat は種数という概念を知らなかったはずだが)であるが，Fermat は

$$X^4 + Y^4 = Z^2 \qquad X \neq 0,\ Y \neq 0 \qquad (**)$$

が整数解をもたないことを示せば十分であることに着目した．この式を

$$(Z/Y^2)^2 = 1+(X/Y)^4$$

の形に書けば，標準形とは異なるけれども楕円曲線である．Fermat に従って，(∗∗)の整数解を考えよう．

(∗∗)が整数解をもったとしよう．そのうちの 1 つ (x,y,z) を

$$\max(|x|,|y|)$$

が正かつ最小になるようにとる(| |は絶対値を表す)． すると，x,y,z は共通因子をもたない．もっと強く 2 つずつ互いに素と仮定してよい．もし，x が奇数ならば，$x^4 \equiv 1 \mod 4$ であるから x,y のうち 1 つは偶数，もう 1 つは奇数でなければならない．したがって，

$$2 \mid x, \quad 2 \nmid y, \quad 2 \nmid z$$

と仮定してよい．(∗∗)を

$$(z+y^2)(z-y^2) = x^4$$

の形に書く．すると，z, y は共に奇数であるから，左辺の 2 因子は共に 2 で割り切れ，またどちらか一方のみ 4 で割り切れる．ゆえに，$z>0$ ととれば次の 2 つの可能性がある．

	第 1 の場合	第 2 の場合
$z+y^2=$	$8u^4$	$2u^4$
$z-y^2=$	$2v^4$	$8v^4$

ただし，$u, v \in \boldsymbol{Z}$ である．第 1 の場合には

$$y^2 = 4u^4 - v^4$$

を得るが，この方程式が整数解をもちえないことは 4 を法として考えればわかる．ゆえに第 2 の場合しか起りえず，

$$y^2 = u^4 - 4v^4$$

を得る．ここで

$$(u^2+y)(u^2-y) = 4v^4$$

であるから

$$u^2+y=2r^4$$
$$u^2-y=2s^4$$

をみたす整数 $r, s\in \boldsymbol{Z}$ が存在する．これから

$$r^4+s^4=u^2$$

を得るが，これは(**)のもう 1 つの解であり，

$$x^4=16u^4v^4=16u^4r^4s^4$$

をみたす．ゆえに $rs\neq 0$ かつ

$$\max(|r|,\ |s|)<|x|\leqq \max(|x|,\ |y|)$$

を得るが，これは解 (x,y,z) の最小性に矛盾する．

対応 $(r,s,u)\to(x,y,z)$ は楕円曲線の 2 倍写像である．つまり，Fermat の降下法(descent)は本質的には Diophantos の上昇法(ascent)の逆である．

2 倍写像が曲線

$$X^4-4Y^4=Z^2$$

を介して 2 ステップに分かれることに注意しよう．この写像は同種写像(isogeny)とよばれるもので次の章で詳しく述べる．

【演習問題】

1　$\boldsymbol{Q}$ 上定義された曲線 $\mathcal{C}$: $Y^2=X^3+AX+B$ を考える．$\boldsymbol{Q}(\sqrt{d})$ は $\boldsymbol{Q}$ の 2 次拡大体で，その非自明な自己同型を $(')$ で表す．$\boldsymbol{x}$ は $\boldsymbol{Q}(\sqrt{d})$ 上定義された $\mathcal{C}$ 上の点とする．$\boldsymbol{x}+\boldsymbol{x}'$ は $\boldsymbol{Q}$ 上定義されること，また $\boldsymbol{x}-\boldsymbol{x}'=(u,v)$ とおけば u と $v/\sqrt{d}$ は $\boldsymbol{Q}$ の元であることを示せ．

$\boldsymbol{Q}(\sqrt{d})$ 上定義される $\mathcal{C}$ 上の点のなす群は $\mathcal{C}$ および曲線 $dY^2=X^3+AX+B$ の $\boldsymbol{Q}$ 上定義される点のなす群から求めることができることを示せ．

2　この問題では $\boldsymbol{Q}$ の 2 次拡大体 $\boldsymbol{Q}(\rho)$, $\rho^3=1$, $\rho\neq 1$ の整数論を仮定している．

次の定理の証明の概略の細部を埋めよ．

定理　$d=q_1q_2$．ただし，$q_1>0$, $q_2>0$ は $q_1\equiv 2\ \ (9)$, $q_2\equiv 5\ \ (9)$ をみたす素数

とする．曲線

$$\mathcal{C}:\ X_1^3+X_2^3+dX_3^3=0$$

の有理点は $(1,-1,0)$ のみである．

［証明の概略］

（i） $\boldsymbol{Q}(\rho)$ 上定義された $\mathcal{C}$ の点は $X_3=0$ をみたすことを証明すれば十分である．

（ii） $\boldsymbol{x}=(x_1,x_2,x_3)$ が $\boldsymbol{Q}(\rho)$ 上定義された $\mathcal{C}$ 上の点であれば一般性を失うことなく，x_1,x_2,x_3 は 2 つごとに $\boldsymbol{Z}[\rho]$ で互いに素となる．

（iii） $(x_1+x_2)(\rho x_1+\rho^{-1}x_2)(\rho^{-1}x_1+\rho x_2)=-q_1q_2x_3^3$．ここで，$\alpha_1,\alpha_2,\alpha_3,\xi_1,\xi_2,\xi_3$ は

$$x_1+x_2=\alpha_1\xi_1^3,\quad \rho x_1+\rho^{-1}x_2=\alpha_2\xi_2^3,$$
$$\rho^{-1}x_1+\rho x_2=\alpha_3\xi_3^3,\qquad \alpha_1\alpha_2\alpha_3=d$$

または

$$x_1+x_2=\lambda\alpha_1\xi_1^3,\quad \rho x_1+\rho^{-1}x_2=\lambda\alpha_2\xi_2^3,$$
$$\rho^{-1}x_1+\rho x_2=\lambda\alpha_3\xi_3^3,\qquad \alpha_1\alpha_2\alpha_3=d$$

をみたす $\boldsymbol{Z}[\rho]$ の元である．ただし，$\lambda=\rho-\rho^{-1}\,[=\sqrt{-3}]$．

（iv） $\alpha_1\xi_1^3+\alpha_2\xi_2^3+\alpha_3\xi_3^3=0,\quad \alpha_1\alpha_2\alpha_3=d$．

（v） 有理的な q_1–進単数は q を法としてある数の 3 乗に等しいが ρ はそうでない．q_2 に関しても同様である．

（vi） （もし必要なら）$\alpha_1,\ \alpha_2,\ \alpha_3$ に ρ または ρ^2 をかけて $\{\alpha_1,\alpha_2,\alpha_3\}$ は $\{\pm1,\pm1,\pm q_1\pm q_2\}$ または $\{\pm1,\pm q_1,\pm q_2\}$ を並べかえたものに等しい．

（vii） 9 を法として考えれば方程式 $\xi_1^3+q_1\xi_2^3+q_2\xi_3^3=0$ は解をもたない(λ^3 を法としても)．

（viii） もし $\{\alpha_1,\alpha_2,\alpha_3\}$ が $\{\pm1,\pm1,\ \pm d\}$ を並べかえたものに等しければ

$$|\xi_1\xi_2\xi_3|_\infty<|x_1x_2x_3|_\infty\,.$$

∎

14

2–同種写像

同種写像(isogeny)とは基礎体上定義された楕円曲線間の写像

$$\mathcal{C} \to \mathcal{D}$$

で $\mathcal{C}$ 上の特別な有理点 $\boldsymbol{o}_\mathcal{C}$ を $\mathcal{D}$ 上の特別な有理点 $\boldsymbol{o}_\mathcal{D}$ にうつすものである．同種写像の核，つまり，$\boldsymbol{o}_\mathcal{D}$ にうつされる点の集合は有限群であり，それら全体は基礎体上定義される．

この章では $\mathcal{C}$ が位数 2 の有理点をもつときを考える．この場合，標準形としては次の形をとるのが便利で，位数 2 の点には $(0,0)$ が対応する．

$$\mathcal{C}:\ \ Y^2 = X(X^2 + aX + b).$$

右辺の 3 次式は重複解をもたないと仮定してあるので

$$b \neq 0, \quad a^2 - 4b \neq 0$$

である．

基礎体を $\boldsymbol{Q}$ とし，$\boldsymbol{x} = (x, y)$ を $\mathcal{C}$ の生成点としよう．つまり，x は超越的で，y は方程式

$$y^2 = x(x^2 + ax + b)$$

により定義されるものとする．体 $\boldsymbol{Q}(x, y)$ は $\mathcal{C}$ の $\boldsymbol{Q}$ 上の**関数体**である．

$$\boldsymbol{x}_1 = \boldsymbol{x} + (0,0)$$

とおく．変換

$$\boldsymbol{x} \to \boldsymbol{x}_1$$

は $\boldsymbol{Q}(x, y)$ の位数 2 の自己同型である．この自己同型の不変体を求めよう．

$(0,0)$ と (x,y) を通る直線を

$$X = tx, \quad Y = ty$$

と表せば $(0,0)$, $\boldsymbol{x}$ および $-\boldsymbol{x}_1 = (x_1, -y_1)$ で $\mathcal{C}$ と交わる．ここで

$$x_1 = b/x,$$
$$y_1 = -by/x^2$$

である．t^2 は明らかに $\boldsymbol{x} \to \boldsymbol{x}_1$ で不変な元であり，それは

$$\begin{aligned} t^2 = (y/x)^2 &= \frac{x^2+ax+b}{x} \\ &= x+x_1+a \end{aligned}$$

である．これを λ とおく．もう 1 つ $\boldsymbol{x} \to \boldsymbol{x}_1$ で不変な元は

$$y+y_1$$

であり，これを μ とおく．

λ と μ の代数的関係式を見つけよう．

$$\begin{aligned} \mu^2 &= y^2(1-b/x^2)^2 \\ &= \frac{x^2+ax+b}{x}(x^2-2b+b^2/x^2) \end{aligned}$$

であるがこの最初の因子は λ にほかならない．2 番目の因子は

$$\begin{aligned} (x+b/x)^2-4b &= (\lambda-a)^2-4b \\ &= \lambda^2-2a\lambda+(a^2-4b) \end{aligned}$$

である．したがって

$$\mu^2 = \lambda(\lambda^2-2a\lambda+(a^2-4b))$$

を得る．

逆に，

$$\lambda^{-1/2}\mu = x-b/x,$$
$$\lambda = x+(b/x)+a$$

であるから，λ, μ と $\lambda^{1/2} = y/x$ を用いて x, y を表せば，

$$x = \frac{1}{2}(\lambda+\lambda^{-1/2}\mu-a), \quad y = \lambda^{1/2}x \tag{$*$}$$

を得る．

$\boldsymbol{Q}(x,y)/\boldsymbol{Q}(\lambda,\mu)$ は 2 次の代数拡大であるから，ガロア理論から $\boldsymbol{Q}(\lambda,\mu)$ が求めるべき不変体となる．

ところで，(λ,μ) は曲線

$$\mathcal{D}:\ Y^2 = X(X^2-2aX+(a^2-4b))$$

の生成点である．

$$\boldsymbol{x}=(x,y)\to\boldsymbol{\lambda}=(\lambda,\mu)$$

から決まる写像

$$\phi:\ \mathcal{C}\to\mathcal{D}$$

は群演算を保つ*1．なぜなら，$\boldsymbol{a},\boldsymbol{b}$ を $\mathcal{C}$ 上の点とし，$f\in\boldsymbol{Q}(\boldsymbol{x})$ は $\boldsymbol{a},\boldsymbol{b}$ で 1 位の極，$\boldsymbol{o}$, $\boldsymbol{a}+\boldsymbol{b}$ で 1 位の零点をもつ関数とする．さらに，f_1 は自己同型 $\boldsymbol{x}\to\boldsymbol{x}_1$ による共役とする．すると，$ff_1\in\boldsymbol{Q}(\boldsymbol{\lambda})$ であり，$\boldsymbol{\lambda}$ の関数として，ff_1 は $\phi(\boldsymbol{a})$, $\phi(\boldsymbol{b})$ で 1 位の極，$\phi(\boldsymbol{o})=\boldsymbol{o}$, $\phi(\boldsymbol{a}+\boldsymbol{b})$ で 1 位の零点をもつ．ゆえに

$$\phi(\boldsymbol{a}+\boldsymbol{b})=\phi(\boldsymbol{a})+\phi(\boldsymbol{b})$$

である．

$\mathcal{D}$ の方程式は $\mathcal{C}$ の方程式とほぼ同じ形をしているので，(λ,μ) と $\mathcal{D}$ に対し同じことを繰り返せば

$$\sigma^2=\rho(\rho^2+4a\rho+16b)$$

をみたす σ, ρ を得る．ここで

$$\xi=\rho/4,\quad \eta=\sigma/8$$

とおけば，$\mathcal{C}$ の生成点を再び得る．

$(\lambda,\mu)=(0,0)$ にうつされる点は $(0,0)$ 以外では 2 等分点である．ゆえに写像 $(x,y)\to(\xi,\eta)$ の核は $\boldsymbol{o}$ と 2 等分点である．したがって，この写像は ± 2 写像である．

同種写像

$$\phi:\ \mathcal{C}\to\mathcal{D}$$

が有理点への影響を考えよう．$\mathcal{C}$, $\mathcal{D}$ の有理点の集合をそれぞれ $\mathfrak{G}$, $\mathfrak{H}$ とし，また，0 でない有理数全体のなす乗法群を $\boldsymbol{Q}^*$ とする．

---

*1　第 24 章補題 1 参照．問題．$f=l+mx+ny$ ならば $ff_1=L+M\lambda+N\mu$ となることを示せ．ただし，$L=l^2-alm+bm^2$, $M=lm-bn^2$, $N=ln$ である．

補題 1　$(u,v)\in\mathfrak{H}$ とする．$(u,v)\in\phi\mathfrak{G}$ となるのは，$u\in(\boldsymbol{Q}^*)^2$ か，$u=0$，$a^2-4b\in(\boldsymbol{Q}^*)^2$ をみたすとき，またそのときに限る．

［証明］　$u\neq 0$ のときは，これは(∗)で $\lambda\to u$，$\mu\to v$ と特殊化して得られる．点 $(\lambda,\mu)=(0,0)$ は点 $(\alpha,0)$ の像(ただし，α は $\alpha^2+a\alpha+b=0$ の解)であるが，$a\in\boldsymbol{Q}$ となるのは $a^2-4b\in(\boldsymbol{Q}^*)^2$ のとき，またそのときに限る．∎

この補題をもとに写像

$$q:\ \mathfrak{H}\to\boldsymbol{Q}^*/(\boldsymbol{Q}^*)^2$$

を以下のように定義する：

$$\begin{aligned} q((u,v)) &= u(\boldsymbol{Q}^*)^2 \qquad (u\neq 0)\\ &= (a^2-4b)(\boldsymbol{Q}^*)^2 \qquad (u=0),\\ q(\boldsymbol{o}) &= (\boldsymbol{Q}^*)^2. \end{aligned}$$

この写像は方程式

$$v^2=u(u^2-2au+a^2-4b)$$

に注意すれば

$$q((u,v))=(u^2-2au+a^2-4b)(\boldsymbol{Q}^*)^2$$

である(ただし，右辺が定義されるときに限る)．

補題 2　写像

$$q:\ \mathfrak{H}\to\boldsymbol{Q}^*/(\boldsymbol{Q}^*)^2$$

は群準同型である．

［証明］　$\mathcal{D}$ の方程式を

$$\mathcal{D}:\ V^2=U(U^2+a_1U+b_1)$$

とおく．$\boldsymbol{u}_j=(u_j,v_j)\in\mathfrak{H}\ (j=1,2,3)$ を

$$\boldsymbol{u}_1+\boldsymbol{u}_2+\boldsymbol{u}_3=\boldsymbol{o}$$

をみたすようにとれば，これらは $\mathcal{D}$ と直線

$$V=lU+m$$

の交点である．これら 2 つの方程式から，

$$\begin{aligned} &U(U^2+a_1U+b_1)-(lU+m)^2\\ &\qquad=(U-u_1)(U-u_2)(U-u_3) \end{aligned}$$

を得る．ゆえに

$$u_1u_2u_3 = m^2$$

であるから，これから $\boldsymbol{u}_j$ $(j=1,2,3)$ のうちどれかが $(0,0)$ である場合を除いて，

$$q(\boldsymbol{u}_1)q(\boldsymbol{u}_2)q(\boldsymbol{u}_3) = (\boldsymbol{Q}^*)^2$$

を得る．

$\boldsymbol{u}_j$ のうち 1 つが $(0,0)$ になっている場合の証明は読者にまかせる．　▮

補題 3　写像

$$q:\ \mathfrak{H} \to \boldsymbol{Q}^*/(\boldsymbol{Q}^*)^2$$

の像は有限群である．

［証明］　一般性を失うことなく

$$a_1 \in \boldsymbol{Z},\quad b_1 \in \boldsymbol{Z}$$

としてよい．$\boldsymbol{Q}^*/(\boldsymbol{Q}^*)^2$ の元は $r(\boldsymbol{Q}^*)^2$（r は平方因子を含まない整数）と書ける．$r|b_1$ となるときのみ $r(\boldsymbol{Q}^*)^2$ が q の像に入ることを示そう．

$q((u,v))=r(\boldsymbol{Q}^*)^2$ とすれば

$$u^2+a_1u+b_1 = rs^2$$
$$u = rt^2$$

をみたす有理数 $s, t\in\boldsymbol{Q}$ が存在する．$t=l/m$，ただし

$$l,\ m\in\boldsymbol{Z},\quad \gcd(l,m)=1$$

とおく．ここで u を消去すれば

$$r^2l^4+a_1rl^2m^2+b_1m^4 = rn^2$$

を得る．ただし $n=m^2s\in\boldsymbol{Z}$ である．

$p|r$，かつ $p\nmid b_1$ をみたす素数 p が存在すると仮定しよう．すると，$p|m$ から $p^2|rn^2$ であり，r は平方因子を含まないから $p|n$ である．ゆえに，$p^3|r^2l^4$ となり，$p|l$ を得るが，これは $\gcd(l,m)=1$ に矛盾する．　▮

これら 3 つの補題を併せて次の定理を得る．

定理 1　$\mathfrak{H}/\phi\mathfrak{G}$ は有限群である．

系　$\mathfrak{G}/2\mathfrak{G}$ は有限群である．

［証明］　次の図式を考える．

$$\begin{array}{ccc} \mathcal{C} & \overset{\times 2}{\rightarrow} & \mathcal{C} \\ \phi \searrow & & \nearrow \psi \\ & \mathcal{D} & \end{array}$$

ここで $\mathfrak{H}/\phi\mathfrak{S}$ と $\mathfrak{S}/\psi\mathfrak{H}$ は有限であり，これから系が従う． ∎

補題 3 の証明で用いた方程式を少し詳しく調べれば（例えば局所的にみれば），$\mathfrak{S}/2\mathfrak{S}$ についてもっと多くの情報が得られる．しかしながら，局所–大域定理はなく，実際，現在においても，解があるかないかを決定するアルゴリズムもないのである．この問題については後の章でまた触れることにしよう．したがって，$\mathfrak{S}/2\mathfrak{S}$ が決定できるような例からいつもそうであるという結論を下すべきではないのである．

まず，何がより詳細にわかるか調べよう．

補題 4　群 $\mathfrak{H}/\phi\mathfrak{S}$ は $\boldsymbol{Q}^*/(\boldsymbol{Q}^*)^2$ の中で以下のような性質をみたすような元 $q(\boldsymbol{Q}^*)^2$ 全体のなす群に同型である．

（i）　$q\in\boldsymbol{Z}$ は平方因子をもたず，$q\,|\,b_1$．

（ii）　方程式

$$ql^4+a_1l^2m^2+(b_1/q)m^4=n^2$$

は $(l,m,n)\neq(0,0,0)$ をみたす整数解をもつ．

さらに $\mathfrak{H}$ の $(0,0)$ は b_1 をその平方因子すべてで割ったものに対応する．□

例 1　以下のような楕円曲線 $\mathcal{C},\mathcal{D}$ を考える：

$$\mathcal{C}:\ Y^2=X(X^2-X+6),$$
$$\mathcal{D}:\ Y^2=X(X^2+2X-23).$$

$\mathfrak{H}/\phi\mathfrak{S}$ の元には，-23 の約数 q が対応する．-23 には $(0,0)$ が対応するので，$q=+23$ か $q=-1$ のうち一方のみを調べればよい．ここでは $q=-1$ のときを調べよう．補題 4 の方程式は

$$-l^4+2l^2m^2+23m^4=n^2$$

つまり，

$$-(l^2-m^2)^2+24m^4=n^2$$

となるが，これは $\boldsymbol{Q}_3$ で考えれば解をもたない．ゆえに $\mathfrak{H}/\phi\mathfrak{S}$ は $(0,0)$ で生

成されることがわかる．

$\mathfrak{G}/\psi\mathfrak{H}$ の元には，6 の約数 q が対応する．ゆえに $q=-1$ または $q=\pm2$, ±3, ±6 である．X^2-X+6 は常に正の値をとるので $q>0$ である．したがって，$q=2, 3$ または 6 であり，特に $q=6$ は $(0,0)$ に対応する．ゆえに $q=2$ または $q=3$ のうち一方を調べればよい．$q=2$ の場合を調べよう．考えるべき方程式は

$$2l^4-l^2m^2+3m^4=n^2$$

であり，これは解 $(l,m,n)=(1,1,2)$ をもつ．これは $(x,y)=(2,4)$ に対応する．

以上より，$\mathfrak{G}/\psi\mathfrak{H}$ は $(0,0)$ と $(2,4)$ で生成されることがわかる．$\mathfrak{G}/2\mathfrak{G}$ の生成元を見つけるには，$\mathfrak{H}/\phi\mathfrak{G}$ の生成元の ψ による像を調べねばならない．この例では $\psi(0,0)=\boldsymbol{o}$ となるので，$\mathfrak{G}/2\mathfrak{G}$ もまた $(0,0)$ と $(2,4)$ で生成されることがわかる．　□

例 2　ここでは Fermat の方程式

$$U^4+V^4=W^4$$

に関係した例を考えよう．

$$Y=V^2W/U^3,\quad X=W^2/U^2$$

とおけば，方程式

$$\mathcal{C}:\ Y^2=X(X^2-1)$$

をみたし，$\mathcal{D}$ の方程式として

$$\mathcal{D}:\ Y^2=X(X^2+4)$$

を得る．

$\mathfrak{H}/\phi\mathfrak{G}$ に対しては，4 の約数 q が対応する．ゆえに $q=-1$, ±2 である．X^2+4 は常に正であるから $q>0$ である．したがって，$q=2$ のときのみ調べればよい．この場合，考えるべき方程式は

$$2l^4+2m^4=n^2$$

であり，これは解 $(l,m,n)=(1,1,2)$ をもつ．これから $\mathfrak{H}/\phi\mathfrak{G}$ の生成元として $(X,Y)=(2,4)$ を得る．$(0,0)$ は $\phi\mathfrak{G}$ に含まれている．

$\mathfrak{G}/\psi\mathfrak{H}$ に関しては，-1 の約数 q が対応する．-1 は $(0,0)$ に対応してお

り，その他の可能性はない．ゆえに $\mathfrak{G}/\psi\mathfrak{H}$ は $(0,0)$ で生成され，$\mathfrak{G}/2\mathfrak{G}$ は $(0,0)$ と $\psi(2,4)=(1,0)$ で生成される． □

【演習問題】

1　以下の曲線に関して

（i）　$\mathfrak{G}/2\mathfrak{G}$ の生成元（ただし $\mathfrak{G}$ は有理点のなす群を表す），

（ii）　位数が 2 のベキ乗である有限位数の元

を求めよ．

$$
\begin{aligned}
Y^2 &= X(X^2+3X+5)\\
Y^2 &= X(X^2-4X+15)\\
Y^2 &= X(X^2+4X-6)\\
Y^2 &= X(X^2-X+6)\\
Y^2 &= X(X^2+2X+9)\\
Y^2 &= X(X^2-2X+9)
\end{aligned}
$$

2　1 と同様な問題を考えて，それを解け．（注意．すべての場合に，$\mathfrak{G}/2\mathfrak{G}$ を求めることはできないが，その大まかな位数はわかる．座標の値が小さいような有理点を探すための，ちょっとしたプログラムを書くには役立つかもしれない．）

3　$\mathcal{C}$: $Y^2=X(X^2+aX+b)$，$\mathcal{D}$: $Y^2=X(X^2+a_1X+b_1)$，$(a_1=-2a,\ b_1=a^2-4b)$ とする．

（i）　有理点のうち，奇数位数の元全体がなす群は同型であることを示せ．

（ii）　有限生成定理を仮定して，有理点のなす群の階数は等しいことを示せ．

（iii）　位数が 2 ベキの元からなる部分群の位数は必ずしも等しくないことを示す例を与えよ．また，どのような可能性があるか決定せよ．

4

（i）　位数が 8 の有理点をもつ楕円曲線を構成せよ．

（ii）　［難しい］位数が 16 の有理点をもつ楕円曲線はないことを示せ．

（iii）　楕円曲線の位数が 2 ベキの有理点全体のなす群を決定せよ．また，おのおのの場合に対しそのような群をもつ楕円曲線の例を与えよ．

5　（もう 1 つの同種写像の例）曲線

$$\mathcal{C}:\ Y^2 = X^3 + B$$

は $\boldsymbol{Q}$ 上定義されているとする．$\beta^2 = B$, $\beta \in \overline{\boldsymbol{Q}}$ とおく．

（i）　直線 $Y = \pm\beta$ は 3 重接線であり，$2(0,\beta) = (0,-\beta)$ となることを示せ．

（ii）　$\boldsymbol{x} = (x, y)$ を生成点とし，

$$\boldsymbol{x}_1 = \boldsymbol{x} + (0,\beta), \quad \boldsymbol{x}_2 = \boldsymbol{x} + (0,-\beta)$$

とおく．このとき

$$\xi = x + x_1 + x_2, \quad \eta = y + y_1 + y_2$$

とおけば，これらは $\boldsymbol{Q}$ 上定義された (x,y) の関数で

$$\mathcal{D}:\ \eta^2 = \xi^3 - 27B$$

をみたすことを示せ．

（iii）　上記の写像をもう 1 度繰り返したものは本質的には 3 倍写像であることを示せ．

（iv）　$\mathfrak{G}, \mathfrak{H}$ はそれぞれ $\mathcal{C}, \mathcal{D}$ の有理点のなす群とする．また $\boldsymbol{Q}(\beta)^*$ は $\boldsymbol{Q}(\beta)$ の 0 でない元のなす乗法群とする．もし $(x,y) \in \mathfrak{G}$ かつ

$$y + \beta \in \{\boldsymbol{Q}(\beta)^*\}^3$$

ならば，$\boldsymbol{x}$ は写像 $\mathcal{D} \to \mathcal{C}$ の $\mathfrak{H}$ の像に含まれることを示せ．

［ヒント．$y + \beta = (u + v\beta)^3$ とおき，β の係数を比較せよ.］

（v）　写像

$$(x,y) \to (y+\beta)\{\boldsymbol{Q}(\beta)^*\}^3$$

は核が $\mathfrak{H}$ の像であるような準同型

$$\mu:\ \mathfrak{G} \to \boldsymbol{Q}(\beta)^* / \{\boldsymbol{Q}(\beta)^*\}^3$$

であることを示せ．

（vi）（代数的整数論の知識が必要）μ の像は有限であることを示せ．

［ヒント．第 15 章参照.］

（vii）　$\mathfrak{G}/3\mathfrak{G}$ は有限群であることを示せ．

15

弱有限生成定理

この章では，楕円曲線

$$Y^2 = F(X),$$

ただし

$$F(X) = X^3 + AX + B, \qquad 4A^3 + 27B^2 \neq 0$$

の有理点のなす群 $\mathfrak{G}$ に対し，$\mathfrak{G}/2\mathfrak{G}$ が有限群であることを証明する．$F(X) = 0$ が有理数解を 1 つもつと仮定した前章と類似した手法を用いる．

ここでは，$F(X)=0$ が有理数解を 3 つもつ場合，1 つもつ場合，まったくもたない場合のどの場合に対しても同じように扱うため，以下では，可換環

$$\boldsymbol{Q}[\Theta] = \boldsymbol{Q}[T]/F(T)$$

上で考える．ただし，T は変数で Θ はその像である．$\boldsymbol{Q}[\Theta]$ は体の直和で，その直和因子の数は $F(T)$ の既約因子の数と同じである[*1]．

ノルム写像

$$\mathrm{N}:\ \boldsymbol{Q}[\Theta] \to \boldsymbol{Q}$$

を次のように定義する：$\alpha \in \boldsymbol{Q}[\Theta]$ として，写像

$$\xi \to \alpha\xi, \qquad \xi \in \boldsymbol{Q}[\Theta]$$

を考えれば，これは $\boldsymbol{Q}[\Theta]$ からそれ自身への写像である．$\boldsymbol{Q}[\Theta]$ を $\boldsymbol{Q}$ 上のベクトル空間とみれば，この写像は線型写像となるので，この写像に対応する

$*1$　前章で $F(T)=0$ が有理数解をもつときの弱有限生成定理を証明したので，$\boldsymbol{Q}[\Theta]$ が体のときに証明すれば十分である．その場合は証明は少し簡単になる．

行列の行列式を $\mathrm{N}(\alpha)$ と定義する．すると

$$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$$

である．$\mathrm{N}(\alpha) \neq 0$ のときに限って α は可逆(つまり，逆元をもつ)である．また，容易にわかるように

$$\mathrm{N}(a-\Theta) = F(a) \qquad (a \in \boldsymbol{Q})$$

である．

$\boldsymbol{Q}[\Theta]^*$ で $\boldsymbol{Q}[\Theta]$ の可逆な元全体のなす乗法群を表すとする．部分群

$$\mathcal{M} \subset \boldsymbol{Q}[\Theta]^*/(\boldsymbol{Q}[\Theta]^*)^2$$

を $\mathrm{N}(\alpha) \in (\boldsymbol{Q}^*)^2$ をみたす元の像全体からなるものとし，写像

$$\mu: \ \mathfrak{G} \to \mathcal{M}$$

を次のように定義する:

（i） $\mu(\boldsymbol{o}) = 1(\boldsymbol{Q}[\Theta]^*)^2$.

（ii） $\boldsymbol{a} = (a, b) \in \mathfrak{G}$, $b \neq 0$ ならば

$$\mu(\boldsymbol{a}) = (a-\Theta)(\boldsymbol{Q}[\Theta]^*)^2.$$

（iii） $\boldsymbol{a} = (a, 0)$ ならば $F(a) = 0$ である．したがって，$\boldsymbol{Q}[\Theta]$ は写像 $\Theta \to a$ からもたらされる $\boldsymbol{Q}$ と同型な直和因子をもつ．この場合，この直和因子では $a-\Theta$ は 0 となる．この場合はこの成分を $\boldsymbol{Q}^*$ の他の元でおきかえて，それにより得られた元の $\boldsymbol{Q}[\Theta]$ でのノルムが $(\boldsymbol{Q}^*)^2$ に含まれるようにしておく．

補題 1　写像 μ は群準同型である．

［証明］　$\mathfrak{G}$ の元 $\boldsymbol{a}_j = (a_j, b_j)$ $(j = 1, 2, 3)$ で

$$\boldsymbol{a}_1 + \boldsymbol{a}_2 + \boldsymbol{a}_3 = \boldsymbol{o}$$

をみたすものとする．つまり，これらは直線

$$Y = lX + m \qquad (l,\ m \in \boldsymbol{Q})$$

上にあるとしてよい．すると，

$$F(X) - (lX+m)^2 = (X-a_1)(X-a_2)(X-a_3)$$

である．X を Θ でおきかえて

$$(a_1-\Theta)(a_2-\Theta)(a_3-\Theta) = (l\Theta+m)^2$$

を得る．$b_j \neq 0$ $(j = 1,\ 2,\ 3)$ ならば $a_1-\Theta$ は可逆であり，補題を得る．

$F(T)$ が可約であり，a_j のうち少なくとも 1 つがその解である場合を考える．$F(T)$ のうちただ 1 つ(e とおく)が a_j たちに含まれるときは，$\boldsymbol{Q}[\Theta]$ は直和 $K_1 \oplus K_2$ または $K_1 \oplus K_2 \oplus K_3$ に分解する．ここで K_1 は $\Theta \to e$ により得られる $\boldsymbol{Q}$ と同型な体である．さて，K_j ($j \neq 1$)成分では，$b_j \neq 0$ ($j=1,2,3$) の場合の証明と同様に考えれば，補題が正しいことがわかる．K_1 成分のとりかえはノルムが常に平方数となるように行なっているので，補題が K_1 成分でも成立することがわかる．

残る場合は b_j がすべて 0 で，a_j がいずれも $F(T)$ の解となっているときである．このとき，$\boldsymbol{Q}[\Theta]$ は $\boldsymbol{Q}$ の 3 つの直和であり，それぞれの直和因子への写像は $\Theta \to a_j$ ($j=1,2,3$) で与えられる．$\Theta - a_1$ の K_2, K_3 成分はそれぞれ $a_2 - a_1$, $a_3 - a_1$ である．したがって，K_1 成分を $(a_2-a_1)(a_3-a_1)(\boldsymbol{Q}^*)^2$ でとりかえれば，直接計算から補題が従う．■

補題 2　μ の核は $2\mathfrak{G}$ である．

［証明］ $\mathcal{M}$ の指数は 2 なので，核は確かに $2\mathfrak{G}$ を含む．これが一致することを示そう．

$$\mu(\boldsymbol{a}) = (\boldsymbol{Q}[\Theta]^*)^2, \quad \boldsymbol{a} = (a, b)$$

としよう．このとき*2,

$$a - \Theta = (p_2\Theta^2 + p_1\Theta + p_0)^2$$

をみたす $p_0, p_1, p_2 \in \boldsymbol{Q}$ が存在する．さらに，$1, \Theta, \Theta^2$ は $\boldsymbol{Q}$ ベクトル空間 $\boldsymbol{Q}[\Theta]$ の基底なので，

$$p_2 \neq 0$$

としてよい．さらに

$$(s_1\Theta + s_0)(p_2\Theta^2 + p_1\Theta + p_0) = r_1\Theta + r_0$$

をみたす有理数 s_0, s_1, r_0, r_1 が存在する．なぜなら右辺の Θ^2 の係数が消えるという条件は，s_0, s_1 に関する線型な条件であるからである．もし $s_1 = 0$, $s_0 \neq 0$ ならば $p_2 = 0$ ということになるので，一般性を失うことなく

$$s_1 = -1$$

*2　$b=0$，つまり $p_2\Theta^2 + p_1\Theta + p_0$ が可逆でないときでも，以下の主張が正しいことは多少の議論が必要．

としてよい．すると，

$$(s_0-\Theta)^2(a-\Theta)=(r_1\Theta+r_0)^2$$

である．Θ を変数 X でおきかえれば，X^3 の係数が 1 であるから

$$(r_1X+r_0)^2-(s_0-X)^2(a-X)=F(X)$$

を得る．

ゆえに直線

$$Y=r_1X+r_0$$

は $Y^2=F(X)$ と (s_0,t) （t はしかるべき有理数）で 2 重に交わり，かつ，もう 1 点 (a,b) または $(a,-b)$ で交わる．これから $(a,b)\in 2\mathfrak{G}$ がわかる． ∎

定理 1　$\mathfrak{G}/2\mathfrak{G}$ は有限群である．

［証明］ 準同型 μ: $\mathfrak{G}\to\mathcal{M}$ の像が有限であることをいえば十分である．一般性を失うことなく

$$A,\ B\in\boldsymbol{Z}$$

としてよい．

$\boldsymbol{x}=(x,y)\in\mathfrak{G}$ としよう．すると，$y^2=F(x)$ から

$$x=r/t^2,\quad y=s/t^3,$$

ただし

$$r,\ s,\ t\in\boldsymbol{Z},\quad \gcd(r,t)=\gcd(s,t)=1$$

かつ

$$s^2=r^3+Art^4+Bt^6$$

をみたすようにとれる．

基本的なアイデアを説明するため，少しの間，$F(X)$ の解 e_1, e_2, e_3 は有理数，したがって整数，と仮定しよう．すると，

$$s^2=(r-e_1t^2)(r-e_2t^2)(r-e_3t^2) \qquad (*)$$

である．

さて，

$$\gcd\{(r-e_1t^2),\ (r-e_2t^2)\}$$

は $(e_1-e_2)t^2$ および $(e_1-e_2)r$ を割り切るので，(e_1-e_2) を割り切る．同様なことは他の因子のペアについてもいえる．したがって，(*)から

$$r-e_j=d_jv_j^2,$$

ここで，d_j は平方因子をもたず，

$$d_j \mid (e_1-e_2)(e_2-e_3)(e_3-e_1),$$

さらに

$$d_1d_2d_3=\text{平方数}$$

をみたす．すると，集合 $\{d_1,d_2,d_3\}$ には有限個の可能性しかなく，これからこの場合の証明を得る．

一般の場合の証明に移る前に，$(v_1,\ v_2,\ v_3,\ t)$ は過剰な方程式系により与えられる曲線

$$\mathcal{D}:\ \begin{cases}(e_1-e_2)t^2 &= d_2v_2^2-d_1v_1^2\\(e_2-e_3)t^2 &= d_3v_3^2-d_2v_2^2\\(e_3-e_1)t^2 &= d_1v_1^2-d_3v_3^2\end{cases}$$

上にあることに注意する．ゆえに，曲線 $\mathcal{D}$ 上に有理点があるかということを調べることにより，$\mathfrak{G}/2\mathfrak{G}$ の情報がわかることもある．

さて，一般の場合を考えよう．$F(X)=0$ の解を $\varepsilon_j\in\overline{\boldsymbol{Q}}\quad(j=1,2,3)$ とおく．そして，$K=\boldsymbol{Q}(\varepsilon_1,\varepsilon_2,\varepsilon_3)$ 上で考えよう[*3]．有理数のときと同様に，イデアル $[r-\varepsilon_1t^2,\ r-\varepsilon_2t^2]$ は $\varepsilon_1-\varepsilon_2$ を割る．したがって，単項イデアル $[r-\varepsilon_jt^2]$ は有限個のイデアル因子の 1 つを除いて，あるイデアルの平方である．類数の有限性と単数群が有限生成であることから，

$$r-\varepsilon_jt^2=\delta_j\lambda_j^2$$

となる．ただし，$\delta_j,\lambda_j\in\boldsymbol{Q}(\varepsilon_j)$ かつ $\{\delta_1,\ \delta_2,\ \delta_3\}$ は有限集合から取り出したものである．これから，μ の像が有限であることがわかり，定理が証明された． ∎

次に $F(X)=0$ の解が有理数のとき，先に述べた曲線 $\mathcal{D}$ に類似した性質をもつ曲線 $\mathcal{D}$ を見つけよう．

すでに示したように，$(x,\ y)\in\mathfrak{G}$ ならば

---

*3　代数的整数論を使うのはここだけである．代数的整数論を知らない読者は有理数体の場合とほぼ同じと思ってよいが，次の脚注も参照のこと．

$$x-\Theta=\delta\lambda^2$$

をみたすような $\boldsymbol{Q}[\Theta]$ の元 δ, λ が存在する．ここで特に，δ は有限集合からとってくることができる．

$$\lambda=v_0+v_1\Theta+v_2\Theta^2 \qquad (v_j\in\boldsymbol{Q})$$

と表せば，右辺は

$$H_0(\boldsymbol{v})+H_1(\boldsymbol{v})\Theta+H_2(\boldsymbol{v})\Theta^2$$

ただし $H_j(\boldsymbol{v})\in\boldsymbol{Q}[\boldsymbol{v}]$ は δ に依存する 2 次形式である．したがって，

$$\mathcal{D}:\ \begin{cases} H_2(\boldsymbol{v})=0 \\ H_1(\boldsymbol{v})=-t^2 \end{cases}$$

上には有理点 $(\boldsymbol{v},t)$ が存在する．

こうして，また $\mathcal{D}$ が局所的にいたるところで解をもつかどうかを調べることにより，$\mathfrak{S}/2\mathfrak{S}$ に関するより多くの情報を得ることができる．もし，そうでなければ，そのような δ はもとの有限集合に含まれてはいないし，もし，$\mathcal{D}$ が局所的にいたるところで解をもてば，2 次曲線

$$H_2(\boldsymbol{v})=0$$

は局所的にいたるところで解をもつ．したがって，第 3 章の定理 1 から $H_2(\boldsymbol{v})=0$ は有理点をもつ．ゆえに(演習問題参照)

$$H_2(\boldsymbol{v})=hL^2-MN$$

と書ける．ただし，h は有理数であり，

$$L(\boldsymbol{v}),\ M(\boldsymbol{v}),\ N(\boldsymbol{v})\ \in\boldsymbol{Q}[\boldsymbol{v}]$$

は 1 次形式である．したがって，$H_2(\boldsymbol{v})=0$ 上の有理点は変数，仮にそれを r, s とおくことにすれば，$\boldsymbol{Q}$ 上の 2 次形式 $V_j(r,s)$ $(j=1,2,3)$ を用いて

$$v_j=V_j(r,s) \qquad (j=1,2,3)$$

と媒介変数表示される．

これから $\mathcal{D}$ は

$$\mathcal{D}':\ t^2=G(r,\ s)$$

(ここで $G(r,s)$ は 2 次形式)に双有理同値であることがわかる．こうすれば代数的整数論という回り道を使うかわりに，2 次形式 G の不変量を使って可

能性のある G の同値類を記述することが可能なこともある*4．事実，これが正に，Birch と Swinnerton-Dyer による有名な結果の中で行なわれていることなのである．[B. J. Birch and H. P. F. Swinnerton-Dyer: Notes on elliptic curves I, II. *J. reine angew. Math.* **212** (1963), 7–25; **218** (1965), 79–108]．

以下，いくつかの例を調べてこの章を終えよう．

例 1

$$Y^2 = X(X^2-1).$$

この例はすでに同種写像の章ですでにでてきたものである．曲線上の点を $(r/t^2, s/t^3)$ とおけば

$$r(r+t^2)(r-t^2) = s^2$$

である．$r-t^2$ と $r+t^2$ の最大公約数は 1 または 2 であり，また r と $r+t^2$ または $r-t^2$ の最大公約数は 1 である．さらに，

$$r+t^2 > r > r-t^2$$

である．したがって，

$$r+t^2 = d_1v_1^2, \quad r = d_2v_2^2, \quad r-t^2 = d_3v_3^2,$$

ただし，d_j は平方数で割り切れないとすれば，起りうる可能性は

$$\begin{aligned}(d_1, d_2, d_3) = &(1,1,1),\\ &(2,1,2),\\ &(1,-1,-1),\\ &(2,-1,-2)\end{aligned}$$

である．これらはすべて位数 2 の点を与え，したがって $\mathfrak{G}/2\mathfrak{G}$ を生成する．□

例 2　さまざまな応用を考える際には代数的整数論が必要な場合が多いが，以下にその 1 例を述べる．この例は後で用いる．

曲線

$$X^3+Y^3+60Z^3 = 0$$

は

$$Y^2 = X^3-3^3(30)^2$$

---

*4　代数的整数論を用いない $\mathfrak{G}/2\mathfrak{G}$ の有限性の証明は，そのかわりとなる 2 元 2 次形式の理論の上に成立しているのである．

に双有理同値である．ここではすべて $\boldsymbol{Q}(\delta)$ ($\delta^3=30$) 上で考えることにする．この体の類数は $h=3$ であり，基本単数は $\eta=1+9\delta-3\delta^2$ である[*5]．

$F(X)=X^3-3^3(30)^2=0$ の解は $3\delta^2$, $3\rho\delta^2$, $3\rho^2\delta^2$ である（ただし，$\rho^3=1$）．従来の表記を用いて，$(r/t^2,\ s/t^3)\in\mathfrak{G}$ とおけば

$$r-3\delta^2t^2,\quad r-3\rho\delta^2t^2,\quad r-3\rho^2\delta^2t^2$$

のうちのどんな組の公約イデアルも $2\cdot3\cdot5$ を割り切らねばならない．2, 3, 5 上で完全に分岐しているので，$r-3\delta^2t^2$ はイデアルの完全平方である．

実数への埋め込みを考えれば，明らかに，

$$r-3\delta^2t^2>0$$

であり，したがって，$r-3\delta^2t^2=\alpha^2$ または $r-3\delta^2t^2=\eta\alpha^2$ をみたす $\boldsymbol{Q}(\delta)$ の元 α がある．

2 番目の可能性が無いことを証明しよう．

$$\alpha=u+v\delta+w\delta^2$$

とおいて，

$$r-3\delta^2t^2=\eta\alpha^2$$

の δ ベキの項の係数をそれぞれ比べれば，

$$0=9u^2+2uv-90v^2-180uw+540vw+30w^2,$$
$$-3t^2=-3u^2+18uv+v^2+2uw-180vw+270w^2.$$

最初の式で

$$u=-28e+90f,$$
$$v=-9e+29f,$$
$$w=g-3e+9f$$

とおけば

$$0=30g^2-4ef$$

である．ゆえに

$$e:f:g=m^2:30n^2:2mn$$

---

*5　この事実をきちんとチェックするのは少々面倒かもしれないが，実際に必要なのは，実数体へ埋め込んだときに $\eta>0$ となることと，η が平方数でないことである．この後半の主張は η をイデアル $[2-\delta,11]$ を法として考えてみればよい．

をみたす整数 m, n が存在もする．これらを 2 番目の方程式に代入すれば，

$$-3l^2 = 3m^4 - 112m^3n + 1620m^2n^2 - 10800mn^3 + 27900n^4$$

をみたす整数 l が存在せねばならないが，これは $\boldsymbol{Q}_2$ で考えれば不可能である．($|n|_2 \leqq |m|_2$ である場合と $|n|_2 > |m|_2$ である場合を分けて考えよ．)

したがって $\mathfrak{G}/2\mathfrak{G}$ は自明な群となる．□

【演習問題】

1　曲線 $Y^2 = F(X)$ で $F(X)$ が以下の場合に位数が 2 ベキの元を決定し，さらに $\mathfrak{G}/2\mathfrak{G}$ の代表系を決定せよ．

(i)　$F(X) = X(X-3)(X+4)$

(ii)　$F(X) = X(X-1)(X+3)$

(iii)　$F(X) = X(X+1)(X-14)$

2

(i)　位数 4 の有理点をもつ楕円曲線の一般形を与えよ．[ヒント．同種写像を用いよ.]

(ii)　楕円曲線は 2 つの独立な位数 4 の有理点($4\boldsymbol{a} = 4\boldsymbol{b} = \boldsymbol{o}$, $2\boldsymbol{a} \neq 2\boldsymbol{b}$, $2\boldsymbol{a} \neq \boldsymbol{o}$, $2\boldsymbol{b} \neq \boldsymbol{o}$ をみたす点 $\boldsymbol{a}, \boldsymbol{b}$)はもたないことを証明せよ．

3　曲線 $Y^2 = F(X)$ で

$$F(X) = (X-e_1)(X-e_2)(X-e_3)$$

($e_j \in \boldsymbol{Q}$)のとき，写像 μ: $\mathfrak{G} \to \mathcal{M}$ の原像を求めるアルゴリズムを考えよ．すなわち，

$$\sigma_j:\ \Theta \to e_j \qquad (j = 1, 2, 3)$$

を $\boldsymbol{Q}[\Theta]$ から $\boldsymbol{Q}$ への準同型とするとき，

(i)　$t_1, t_2, t_3 \in \boldsymbol{Q}$ が与えられたとき，

$$\sigma_j(\lambda) = t_j \qquad (j = 1, 2, 3)$$

をみたすような $\lambda = l_0 + l_1\Theta + l_2\Theta^2$ $(l_j \in \boldsymbol{Q})$ を求めよ．また，そのような λ は一意的であることを示せ．

(ii)

$$x - e_j = t_j^2 \qquad (j = 1, 2, 3)$$

をみたす有理数 x に対し，(i)で構成した λ は $\lambda^2 = x - \Theta$ をみたすことを示せ．

(iii) t_j, e_j を用いて表される $\boldsymbol{Q}$ の元 s_0 で，例えば

$$(s_0-\Theta)\lambda = r_0+r_1\Theta$$

とおいたとき，Θ^2 の項が消えるものを見つけよ．

(iv) 適当な $\boldsymbol{Q}$ の元？に対して $(x, t_1t_2t_3)=2(s_0, ?)$ となることを示せ．

(v) t_j を $\pm t_j$ とおきかえて $2\boldsymbol{x}_1=\boldsymbol{x}$ をみたすもう 1 つの $\boldsymbol{x}_1$ が得られることを示せ．また，異なる $\boldsymbol{x}_1$ どうしの関係は何か．

(vi) 上で求めたことを用いて，$F(X)=X(X-3)(X+5)$ と $\boldsymbol{x}=(4,6)$ のときに $2\boldsymbol{x}_1=\boldsymbol{x}$ をみたす $\boldsymbol{x}_1$ をすべて求めよ．

4 [Fermat, Euler] 標準形に変換するか，その他の方法を用いて，曲線

$$X_1^2-2X_2^2+X_3^2=0, \quad X_2^2-2X_3^2+X_4^2=0$$

上の有理点 (x_1, x_2, x_3, x_4) は $x_1^2=x_2^2=x_3^2=x_4^2$ をみたすものに限ることを示せ．

整数 $n_1<n_2<n_3<n_4$ が等差数列をなすとき，それらがすべて平方数ということはありえないことを示せ．

16

補足：終結式

最近は代数学の講義などで終結式や判別式に関して述べられることはあまりないので，ここでこれらに関してまとめておこう．基礎体は任意の体とする．

$$F(X) = f_n X^n + f_{n-1} X^{n-1} + \cdots + f_0,$$
$$G(X) = g_m X^m + g_{m-1} X^{m-1} + \cdots + g_0$$

とする．多項式系

$$\left.\begin{array}{c} F(X) \\ XF(X) \\ \vdots \\ X^{m-1}F(X) \\ G(X) \\ \vdots \\ X^{n-1}G(X) \end{array}\right\} \qquad (*)$$

は，$m+n$ 個の変数 $X^{m+n-1}, \cdots, 1$ に関する $m+n$ 個の 1 次形式とみなせる（つまり，忘却関手である）．この $m+n$ 個の 1 次形式から得られる $m+n$ 次正方行列の行列式 $R(F, G)$ は F, G の**終結式**とよばれる．$R(F, G)$ は符号を除いて定まる．

$X^{m+n-1}, \cdots, X$ を消去して $R(F, G)$ を（$*$）の列で表す:

$$A(X)F(X)+B(X)G(X)=R(F,G) \tag{1}$$

ここで $A(X)$, $B(X)$ はそれぞれ，次数が $\leqq m-1$, $\leqq n-1$ である．ここで F, G の係数が，例えば $\boldsymbol{Z}$ に含まれるならば $R(F, G)\in\boldsymbol{Z}$ であり，$A(X)$, $B(X)\in\boldsymbol{Z}[X]$ である．

もし，$F(X)$, $G(X)$ が代数閉包まで込めて考えたときに共通解 x をもてば，(1)から $R(F, G)=0$ が従う．逆に，$R(F,G)=0$ とするとき，(*)は非自明な1次関係を与えており，したがって

$$A(X)F(X)+B(X)G(X)=0$$

をみたす次数がそれぞれ $\leqq m-1, n-1$ で共には0にならない多項式 $A(X)$, $B(X)$ が存在する[*1].

$F(X)$, $G(X)$ の次数がちょうど n, m（つまり，$f_n\neq0$, $g_m\neq0$）ならば，$F(X)$ と $G(X)$ は共通因子をもち，これから代数閉包の中で共通解をもつことがわかる．

もし，$f_n=g_m=0$ ならば明らかに $R(F,G)=0$ である．また，もし，$f_n\neq 0$ で，$g_m=0$ ならば，

$$R(F,G)=f_nR(F,G^*),$$

ただし，

$$G^*=g_{m-1}X^{m-1}+\cdots+g_0$$

である．したがって，より精密にまとめれば以下のようになる：同次式

$$f_nX^n+f_{n-1}X^{n-1}U+\cdots+f_0U^n,$$
$$g_mX^m+\cdots+g_0U^m$$

が代数閉包で共通解 $(x,u)\neq(0,0)$ をもつ必要十分な条件は，$R(F,G)=0$ となることである．

非斉次な多項式にもどって

$$F(X)=f_n\prod_j(X-\theta_j),$$

$$G(X)=g_m\prod_k(X-\phi_k)$$

*1　(1)を与えるような消去法により得られる特別な $A(X)$, $B(X)$ についてはもちろん共に0かもしれない．

とおく．$f_n, g_m, \theta_1, \cdots, \theta_n, \phi_1, \cdots, \phi_m$ を変数と考えれば，$R(F,G)$ はそれらの多項式であり，θ_j のどれかが ϕ_k のどれかに等しければそれは 0 である．したがって次数を考慮すれば

$$\begin{aligned}R(F,G) &= \pm f_n^m g_m^n \prod_{j,k} (\theta_j - \phi_k)\\ &= \pm f_n^m \prod G(\theta_j)\\ &= \pm g_m^n \prod F(\phi_k)\end{aligned}$$

となる．$H = H(X)$ をもう 1 つの多項式とすると，上で考えたことから

$$R(F,GH) = \pm R(F,G)R(F,H)$$

が従う．さらに G_1, G_2 が共に次数 m で $G_1 - G_2$ が F で割り切れれば，

$$R(F,G_1) = \pm R(F,G_2)$$

が成り立つ．最後に $G = F'$，(形式的な)微分，とおくと，

$$F'(\theta_i) = f_n \prod_{j \neq 1} (\theta_i - \theta_j)$$

であるから

$$R(F,F') = \pm f_n^{2n-1} \prod_{i<j} (\theta_i - \theta_j)^2$$

が成立する．右辺の $+$ の方をとった関数は**判別式** $D(F)$ であり，それは F が重解をもつときに限り 0 になる．

例えば，$F(X) = X^3 + AX + B$ のときは $D = 4A^3 + 27B^2$ であり，(1)は

$$\begin{aligned}&(6AX^2 - 9BX + 4A^2)(3X^2 + A) - (18AX - 27B)(X^2 + AX + B)\\ &\quad = 4A^3 + 27B^2\end{aligned}$$

である．

【演習問題】

1　$F(X) \in \boldsymbol{Z}_p[X]$ が判別式 D をもち，$a \in \boldsymbol{Z}_p$ とする．

$$|F(a)|_p < |D|_p$$

ならば $|F'(a)|_p \geqq |D|_p$ が成立することを示せ．

17

高さと有限基底定理の証明

この章では“高さ”の概念を導入し，有限基底定理の証明を完結しよう．

$\boldsymbol{u}=(u_0,\cdots,u_n)$ を $\boldsymbol{Q}$ 上の n 次元射影空間の点とする．同次座標を用いていることを考慮すれば，一般性を失うことなく，

$$u_j \in \boldsymbol{Z}, \quad \gcd(u_0,\cdots,u_n)=1 \tag{1}$$

と仮定してよい．このような正規化をした後，$\boldsymbol{u}$ の**高さ** $\boldsymbol{H}(\boldsymbol{u})$ を

$$\boldsymbol{H}(\boldsymbol{u})=\max_j |u_j|$$

と定義する．この章では $|\ \ |$ は絶対値($|\ \ |_\infty$)を表す．

ここでは主に射影直線の点の高さを考える．$x\in\boldsymbol{Q}$ を射影直線上の点 $(x,1)$ と同一視し，$x=u_0/u_1$, u_0, $u_1\in\boldsymbol{Z}$ と既約分数の形に表せば，

$$\boldsymbol{H}(x)=\max\{|u_0|,\ |u_1|\}$$

である．

補題 1

（i） $D(U_0, U_1)$, $E(U_0,U_1)$ $(\in \boldsymbol{Q}[U_0, U_1])$ は共に次数が n の同次式とする．$\boldsymbol{u}=(u_0, u_1)$ を $\boldsymbol{Q}$ 上定義された射影直線の有理点で，$D(\boldsymbol{u})$ と $E(\boldsymbol{u})$ は共通零点はもたないとする．このとき

$$\boldsymbol{H}(D(\boldsymbol{u}),\ E(\boldsymbol{u}))\leqq c\boldsymbol{H}(\boldsymbol{u})^n$$

（ただし，c は $\boldsymbol{u}$ に依存しない数）が成立する．

（ii） さらに，D と E の終結式が 0 でないと仮定する．すると

$$\boldsymbol{H}(D(\boldsymbol{u}),\, E(\boldsymbol{u})) \geqq \gamma \boldsymbol{H}(\boldsymbol{u})^n$$

をみたす $\boldsymbol{u}$ に依存しない数 $\gamma > 0$ が存在する． □

注意 (ii)の付加条件は D, E が代数閉包 $\overline{\boldsymbol{Q}}$ で共通解をもたないことに同値である．

［証明］ 同次性を用いれば，

$$D(U_0,\, U_1),\ E(U_0,\, U_1) \in \boldsymbol{Z}[U_0,\, U_1]$$

かつ $\boldsymbol{u} = (u_0,\, u_1)$ は(1)のように正規化されているとしてよい．また

$$|D(\boldsymbol{u})|,\ |E(\boldsymbol{u})| \leqq c\{\max(|u_0|,\, |u_1|)\}^n$$

が成り立つような c が存在するのは明らかである．これから(i)が従う．

次に，(ii)の仮定が成り立つとする．R で終結式を表すとき，

$$L_j D + M_j E = R U_j^{2n-1} \qquad (j = 0, 1) \tag{$*$}$$

をみたす同次形式 $L_j(U_0,\, U_1),\ M_j(U_0,\, U_1) \in \boldsymbol{Z}[U_0,\, U_1]$ $(j = 0, 1)$ が存在する．$\boldsymbol{U}$ に $\boldsymbol{u}$ を代入すれば

$$\gcd\{D(\boldsymbol{u}),\, E(\boldsymbol{u})\} \mid R$$

が得られる．

さらに，(i)の証明同様，

$$|L_j(\boldsymbol{u})|,\ |M_j(\boldsymbol{u})| \leqq c'\{\max(|u_0|,\, |u_1|)\}^{n-1} \qquad (j = 0, 1)$$

が成り立つような c' が存在する．($*$)に代入($\boldsymbol{U}$ に $\boldsymbol{u}$ を)して，$\gamma = 1/2c'$ とおけば，(ii)が得られる． ∎

さて，$\boldsymbol{u}, \boldsymbol{v}$ を射影直線上の 2 点とし

$$\begin{aligned}\boldsymbol{w} &= (u_0 v_0,\, u_0 v_1 + u_1 v_0,\, u_1 v_1) \\ &= (w_0,\, w_1,\, w_2)\end{aligned}$$

とおく．このとき次の補題が成立する．

補題 2

$$\frac{1}{2} \leqq \frac{\boldsymbol{H}(\boldsymbol{w})}{\boldsymbol{H}(\boldsymbol{u})\boldsymbol{H}(\boldsymbol{v})} \leqq 2\,.$$

［証明］ $\boldsymbol{u}, \boldsymbol{v}$ が(1)により正規化されているとすれば，右側の不等式はただちに従う．

$w_0,\, w_1,\, w_2$ が共通な因子を含まないのは簡単にわかるので

$$\max(|w_0|,\ |w_1|,\ |w_2|) \geqq \frac{1}{2}\{\max(|u_0|,\ |u_1|)\}\{\max(|v_0|,\ |v_1|)\}$$

を示せば十分であるが，これは読者に演習問題として残しておこう．　∎

楕円曲線

$$\mathcal{C}:\ Y^2 = X^3 + AX + B, \qquad A,\ B \in \boldsymbol{Z}, \quad 4A^3 + 27B^2 \neq 0$$

にもどろう．$\mathcal{C}$ 上の有理点 $\boldsymbol{x} = (x, y)$ の高さ $H(\boldsymbol{x})$ を x–座標の高さ $\boldsymbol{H}(x)$ と定義するのが有効であり，またそれが通例である．すなわち，$\boldsymbol{x} = (x,\ y,\ z)$ を同次座標とするならば

$$H(\boldsymbol{x}) = \boldsymbol{H}(x, z), \qquad (\boldsymbol{x} \neq \boldsymbol{o})$$
$$H(\boldsymbol{o}) = 1$$

である．

補題 3

$$\gamma_1 \leqq \frac{H(2\boldsymbol{x})}{H(\boldsymbol{x})^4} \leqq c_1$$

をみたす $\mathcal{C}$ のみに依存する定数 $c_1, \gamma > 0$ が存在する．

［証明］　$\boldsymbol{x} = (x,\ y)$，$2\boldsymbol{x} = (x_2,\ y_2)$ とおけば，

$$x_2 = D(x)/E(x),$$

ただし，

$$D(x) = (3x^2 + A)^2 - 8x(x^3 + Ax + B),$$
$$E(x) = 4(x^3 + Ax + B)$$

である．ここで $3x^2 + A$ と $x^3 + Ax + B$ の終結式は $4A^3 + 27B^2 \neq 0$ であることと，前章の公式から $D(x)$ と $E(x)$ の終結式 R は $(4A^3 + 27B^2)^2$ の 4 ベキ倍となる．したがって補題 1 を $x \fallingdotseq u_0/u_1$，$n = 4$ として適用すれば，補題が従う[*1]．　∎

補題 4　$\boldsymbol{x}_1, \boldsymbol{x}_2$ は $\mathfrak{G}$ の元とする．すると

$$H(\boldsymbol{x}_1 + \boldsymbol{x}_2)H(\boldsymbol{x}_1 - \boldsymbol{x}_2) \leqq c_2 H(\boldsymbol{x}_1)^2 H(\boldsymbol{x}_2)^2$$

＊1　実際，補題 1 の証明をこの場合に当てはめて考えれば，L_j，M_j で $4A^3 + 27B^2$ が打ち消しあうので，R の代わりに $4A^3 + 27B^2$ をとってよい．第 12 章の終りの公式(＊)を参照のこと．詳しい公式は巻末に紹介してある Silverman の本を参照．

が成立する．ここで c_2 は $\mathcal{C}$ のみに依存する数である．

［証明］ $$\boldsymbol{x}_1+\boldsymbol{x}_2=\boldsymbol{x}_3, \quad \boldsymbol{x}_1-\boldsymbol{x}_2=\boldsymbol{x}_4$$

と書いて，$\boldsymbol{x}_j=(x_j, y_j)$ とおけば射影平面の元として

$$(1, x_3+x_4, x_3x_4)=(W_0, W_1, W_2)$$

を得る．ただし

$$\begin{aligned} W_0 &= (x_2-x_1)^2 \\ W_1 &= 2(x_1x_2+A)(x_1+x_2)+4B \\ W_2 &= x_1^2x_2^2-2Ax_1x_2-4B(x_1+x_2)+A^2 \end{aligned}$$

である（巻末の公式集参照）．x_1, x_2 を整数の商の形に表して同次化すれば

$$\boldsymbol{H}(W_0, W_1, W_2) \leqq c_3\boldsymbol{H}(x_1)^2\boldsymbol{H}(x_2)^2$$

をみたすような c_3 が存在することがわかる．一方，補題 2 から，

$$\begin{aligned} \boldsymbol{H}(W_0, W_1, W_2) &= \boldsymbol{H}(1, x_3+x_4, x_3x_4) \\ &\geqq \frac{1}{2}\boldsymbol{H}(x_3)\boldsymbol{H}(x_4) \end{aligned}$$

である．$c_2=2c_3$ とおけば，補題 4 が得られる． ∎

系

$$\min(H(\boldsymbol{x}_1+\boldsymbol{x}_2), H(\boldsymbol{x}_1-\boldsymbol{x}_2)) \leqq c_4H(\boldsymbol{x}_1)H(\boldsymbol{x}_2)$$

ただし，$c_4=c_2^{1/2}$ である． □

また，一方で次の補題が成立する．

補題 5 正数 λ が与えられたとき，$\boldsymbol{x}\in\mathfrak{G}$ で $H(\boldsymbol{x})\leqq\lambda$ をみたすものは有限個に限る．

［証明］ $\boldsymbol{x}=(x, y)$ が $\boldsymbol{H}(\boldsymbol{x})\leqq\lambda$ をみたすことから，$x=u_0/u_1$, $u_0, u_1\in\boldsymbol{Z}$ と書けば，$|u_0|, |u_1|\leqq\lambda$ となる．これから有限性が従う． ∎

これで次の定理を証明する準備が整った．

有限基底定理 有理点のなす群 $\mathfrak{G}$ は有限生成である．

［証明］ “弱” 有限生成定理（第 15 章の定理 1）から，$\mathfrak{G}/2\mathfrak{G}$ は有限である．$\boldsymbol{b}_1, \cdots, \boldsymbol{b}_s\in\mathfrak{G}$ を $2\mathfrak{G}$ を法とする代表系とする．$\boldsymbol{a}\in\mathfrak{G}$ とすれば，$\boldsymbol{a}+\boldsymbol{b}_j$, $\boldsymbol{a}-\boldsymbol{b}_j$ が共に $2\mathfrak{G}$ の元となるような j がとれる．補題 4，系からどちらか一方の符

号に対しては

$$H(\boldsymbol{a}\pm\boldsymbol{b}_j) \leqq c_4 H(\boldsymbol{a})H(\boldsymbol{b}_j)$$

となる(訳者注．ここで符号は不等式をみたす方をとる)．

ここで $\boldsymbol{a}\pm\boldsymbol{b}_j=2\boldsymbol{c}$, $\boldsymbol{c}\in\mathfrak{G}$ (符号は不等式をみたす方を選ぶものとする)とおけば，補題3から，

$$H(\boldsymbol{a}\pm\boldsymbol{b}_j) \geqq \gamma_1 H(\boldsymbol{c})^4$$

である．まとめれば，

$$\begin{aligned} H(\boldsymbol{c})^4 &\leqq \gamma_1^{-1} c_4 H(\boldsymbol{a})H(\boldsymbol{b}_j) \\ &\leqq \kappa H(\boldsymbol{a}) \end{aligned}$$

である．ただし

$$\kappa = \gamma_1^{-1} c_4 \max_j H(\boldsymbol{b}_j)\,.$$

ゆえに，

$$H(\boldsymbol{c}) \leqq \frac{1}{2} H(\boldsymbol{a})$$

または

$$H(\boldsymbol{a}) \leqq (16\kappa)^{1/3} \ (=\lambda \text{ とおく})$$

である．以上から，$\mathfrak{G}$ は $\boldsymbol{b}_j$ と $H(\boldsymbol{a})\leqq\lambda$ をみたす $\boldsymbol{a}$ で生成されることがわかるが，補題5からそのような $\boldsymbol{a}$ は有限個である． ∎

高さの性質を簡単にまとめて，この章を終えよう．

補題4の性質に関しては，反対方向の不等式，つまり

$$H(\boldsymbol{x}_1+\boldsymbol{x}_2)H(\boldsymbol{x}_1-\boldsymbol{x}_2) \geqq \gamma_2 H(\boldsymbol{x}_1)^2 H(\boldsymbol{x}_2)^2 \qquad (*)$$

が成立する．ただし，γ_2 は正の定数である．実際，補題4の証明で，W_0, W_1, W_2 を不定元 x_1, x_2 の関数と考えれば，これらは代数閉包の中で共通解をもたない．なぜなら，$W_0=0$ から $x_2=x_1$ であるが，このとき，W_1 と W_2 は補題3の証明で用いた関数 D, E になるからである．すると，(*)は補題1を適当に一般化したものから従う．こうなると補題3は拡張された補題4で，$\boldsymbol{x}_2=\boldsymbol{x}_1$ であることに注意しよう．

次に，**対数的高さ**(logarithmic height)

$$h(\boldsymbol{x}) = \log H(\boldsymbol{x})$$

を考える．拡張された補題4を用いれば，

$$|h(\boldsymbol{x}_1+\boldsymbol{x}_2)+h(\boldsymbol{x}_1-\boldsymbol{x}_2)-2h(\boldsymbol{x}_1)-2h(\boldsymbol{x}_2)| \leqq c$$

をみたす定数 c が存在する．特に，

$$|h(2\boldsymbol{x})-4h(\boldsymbol{x})| \leqq c$$

が成立する．これから極限

$$\hat{h}(\boldsymbol{x}) = \lim_{n\to\infty} h(2^n\boldsymbol{x})/4^n$$

が存在すること，および，それが

$$\hat{h}(\boldsymbol{x}_1+\boldsymbol{x}_2)+\hat{h}(\boldsymbol{x}_1-\boldsymbol{x}_2) = 2\hat{h}(\boldsymbol{x}_1)+2\hat{h}(\boldsymbol{x}_2)$$

をみたすことが従う．こうなれば，

$$\hat{h}(\boldsymbol{x}_1+\boldsymbol{x}_2)-\hat{h}(\boldsymbol{x}_1)-\hat{h}(\boldsymbol{x}_2)$$

が $\boldsymbol{x}_1$，$\boldsymbol{x}_2$ に関して双線型であり，したがって $\hat{h}(\boldsymbol{x})$ は $\mathfrak{G}$ 上の2次形式であることを証明するのは簡単な演習問題(演習問題参照)であろう．関数 $\hat{h}(\boldsymbol{x})$ は**標準的高さ**[*2](canonical height)とよばれるものである．特に，

$$\hat{h}(n\boldsymbol{x}) = n^2\hat{h}(\boldsymbol{x})$$

であり，これから $\boldsymbol{x}$ が有限位数の元ならば $\hat{h}(\boldsymbol{x})=0$ であることがわかる．逆は補題5と $h(\boldsymbol{x})-\hat{h}(\boldsymbol{x})$ が有界であることから従う．

【演習問題】

1

(i)　$a\in \boldsymbol{Q}$，$a\neq 0$ とする．このとき，有限個の素数 p を除いて $|a|_p=1$ であり，

$$\prod_{p\,\mathrm{inc}\,\infty} |a|_p = 1$$

であることを示せ．

(ii)　$u_0,\cdots,u_n\in \boldsymbol{Q}$ ですべてが0ではないとする．このとき，有限個の素数 p

*2　標準的高さの定義には異なったものがある．それらは定数倍を除いて等しい．

を除けば $\max|u_j|_p=1$ であり,

$$\prod_{p \operatorname{inc} \infty} \max_j |u_j|_p = \boldsymbol{H}(\boldsymbol{u})$$

は射影空間の点 $\boldsymbol{u}=(u_0, \cdots, u_n)$ の高さになることを示せ.

2　（本文への補足） $f(x)$ は加法群 $\mathfrak{M}$ の元 x に関して定義された関数で標数 $\neq 2$ の体で値をとるものとする. $\mathfrak{M}$ の任意の元 x, y に対して

$$f(x+y)+f(x-y) = 2f(x)+2f(y)$$

が成り立つとき,

$$f(x) = B(x,\ x)$$

をみたす適当な対称な双線型形式 $B(x,\ y)$ が存在することを示せ.

［ヒント.
$$B(x,\ y) = \frac{1}{2}\{f(x+y)-f(x)-f(y)\}$$

とおいて

$$B(x+z,\ y) = B(x,\ y)+B(z,\ y)$$

が成り立つことを示せばよい. つまり,

$$f(x+y+z)+f(x)+f(y)+f(z) = f(y+z)+f(z+x)+f(x+y).$$

まず手始めに

$$(x+y+z)+x = (x+z)+(y+z)$$

を調べよ.］

3　$\mathcal{C}$: $Y^2=X^3+AX+B$ とし, $\boldsymbol{x}_1, \boldsymbol{x}_2$ は独立な生成点とする. $\boldsymbol{x}_3=\boldsymbol{x}_1+\boldsymbol{x}_2$, $\boldsymbol{x}_4=\boldsymbol{x}_1-\boldsymbol{x}_2$ とおく.

$$(x_1-x_2)^2(x_1+x_2+x_3) = (y_1-y_2)^2,$$
$$(x_1-x_2)^2(x_1+x_2+x_4) = (y_1+y_2)^2.$$

$x_1+x_2+x_3$, $x_1+x_2+x_4$ は方程式

$$(x_1-x_2)^2T^2+uT+v = 0$$

の解であることを示せ. ただし, u, v は x_1, x_2 に関する**多項式**である.

x_3, x_4 に関して同様の結果を示せ.

4　（本文への補足）$G(\boldsymbol{X}) \in \boldsymbol{Q}[\boldsymbol{X}]$ は $\boldsymbol{X}=(X, Y, Z)$ に関する非特異な 2 次形式とし, $G(\boldsymbol{x})=0$ をみたす $\boldsymbol{x}=(x, y, z) \neq (0,0,0)$ が存在すると仮定する.

$$G(\boldsymbol{X}) = L(\boldsymbol{X})M(\boldsymbol{X})+dN(\boldsymbol{X})^2$$

をみたす線型形式 $L(\boldsymbol{X})$, $M(\boldsymbol{X})$, $N(\boldsymbol{X}) \in \boldsymbol{Q}[\boldsymbol{X}]$ と $d \in \boldsymbol{Q}^*$ が存在することを示せ.

［ヒント.

（i） 一般性を失うことなく，$\boldsymbol{x}=(1,0,0)$ としてよい．

（ii） Y, Z に関する線型変換の後，$G(\boldsymbol{X})=XY+Y, Z$ に関する形式，と仮定してよい．

（iii） Z に関して完全平方をとれ．］

5 $\hat{h}$ は曲線 C 上の標準的高さとし，$\mathfrak{G}/2\mathfrak{G}$ の代表系がすべて $\hat{h}(\boldsymbol{x})\leqq t$ をみたすような t がとれるものとする．$\mathfrak{G}$ は $\hat{h}(\boldsymbol{a})\leqq t$ をみたすような元 $\boldsymbol{a}$ で生成されることを示せ．

18

種数が1の曲線に関する局所–大域原理

さて，楕円曲線から一般の種数1の曲線へ注意をうつそう．この章では種数1の曲線については局所–大域原理が成立しない例を与える．そして後の章で，局所–大域原理の“障害”，すなわち，Tate–Shafarevich 群について述べよう．

ここで扱う例は，Selmer による

$$3X^3+4Y^3+5Z^3=0 \tag{1}$$

と Lind と Reichardt がそれぞれ独立に研究した

$$X^4-17=2Y^2 \tag{2}$$

である．これまで述べてきたことを用いれば，有理点が存在しないことを証明するのは可能であるが，局所的にいたるところで有理点が存在することを証明する手立ては述べてない．これは第25章まで有限体上の楕円曲線の議論を残しているからである．もちろん p が与えられれば，$\boldsymbol{Q}_p$ 上の有理点の存在は確認できるかもしれないが，それが(1)または(2)が $\boldsymbol{Q}_P$ で解をもたないような P──例えば，$P>10^{10}$ をみたすような P──が存在する可能性を完全に打ち消しているわけではない．ここではとりあえず，有限体 $\boldsymbol{F}_p$ 上定義された楕円曲線が常に $\boldsymbol{F}_p$–有理点をもつ(第25章定理2)という事実を仮定しよう．すると，(1)および(2)の p を法とする還元がまた種数1であれば，第10章の補題1より，その点は $\boldsymbol{Q}_p$ 上まで持ち上げることができる．この事

実を用いれば[*1]，(1)に関しては考えるべき $\boldsymbol{Q}_p$ は $p=2,3,5$ に対してであり，(2)に関しては $p=2,17$ であることがわかる．これらの p に対して各曲線が解をもつことを確認するのは読者にまかせることにしよう．

曲線(1)に関して，有理点が存在しないことを示すのには次の補題を用いる．

補題 1 a, b, c は 1 より大きい相異なる整数とし，$d=abc$ は 3 乗の因子を含まないとする．また，

$$au^3+bv^3+cw^3=0$$

をみたす整数 $u, v, w, uvw\neq 0$ が存在すると仮定する．このとき，

$$x^3+y^3+dz^3=0$$

をみたす整数 $x, y, z\,(z\neq 0)$ が存在する．

［証明］ $\rho^3=1,\ \rho\neq 1$ とし

$$\xi = au^3+\rho bv^3+\rho^2 cw^3$$
$$\eta = au^3+\rho^2 bv^3+\rho cw^3$$

とおくと

$$\xi+\eta = 3au^3$$
$$\rho\xi+\rho^2\eta = 3cw^3$$
$$\rho^2\xi+\rho\eta = 3bv^3$$

であり，したがって，

$$\xi^3+\eta^3+d\zeta^3=0, \quad \zeta=-3uvw$$

を得る．ここで，2 点 $(\xi,\ \rho\eta, \zeta)$，$(\eta,\ \rho^2\xi,\ \zeta)$ は $\boldsymbol{Q}$ 上共役である．ゆえに，この 2 点を結ぶ直線は $X^3+Y^3+dZ^3=0$ と $(1,\ -1,\ 0)$ と異なる $\boldsymbol{Q}$ 上定義された点で交わる． ∎

補題 2 曲線

$$X^3+Y^3+60Z^3=0$$

の $\boldsymbol{Q}$ 上の有理点は $(1,-1,0)$ のみである．

---

*1 (1)，(2)も含めてこれはよく初等的に証明される．例えば，A. Weil: Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.* **55** (1949), 497–508 (全集 I，395–410)参照．

［証明］　位数有限の元がないことは，例えば3次曲線の例外点（第6章補題1）からわかる．さて，問題の曲線は $\boldsymbol{Q}$ 上

$$Y^2 = X^3 - 2^4 \cdot 3^3 \cdot 60^2$$

に双有理同値である．弱有限生成定理の章の終りの部分（第15章2つめの例）から，この後の曲線については $\mathfrak{G}/2\mathfrak{G}$ は自明である．すると，有限基底定理から $\mathfrak{G}$ が自明であることが従う．∎

定理1　曲線（1）上には有理点は存在しない．

［証明］　先の2つの補題から従う．∎

ここまでの話しでは代数的数も用いたが，次の定理の証明は有理数の範囲のみでできる．

定理2　曲線（2）上に有理点は存在しない．

［証明］　有理点 (x, y) が（2）の上に存在するとしよう．$x=a/c$ と既約分数の形に書いておく．すると，

$$a^4 - 17c^4 = 2b^2,$$
$$\gcd(a,c) = \gcd(b,c) = \gcd(a,b) = 1$$

となる．

$$A = a^2, \quad C = c^2$$

とおけば

$$A^2 - 17C^2 = 2b^2$$

を得る．この方程式は局所的にいたるところで解けるので，大域的に解をもつ．実際，

$$5^2 - 17 \cdot 1^2 = 2 \cdot 2^2$$

である．これから

$$(5A+17C+4b)(5A+17C-4b) = 17(A+5C)^2$$

を得る．左辺の2つの因子が共通な奇素数で割り切れれば，その奇素数は $5A+17C$ と $A+5C$ の約数である．したがって $8A$ と $8C$ を割り切る．これは矛盾である．左辺の2つの因子は同じ符号をもち，$A=a^2$, $C=c^2$ は正である．したがって，u, v を適当な整数とすれば次の2つの可能性がある．

$$
\begin{array}{rcll}
 & & \text{第 1 の場合} & \text{第 2 の場合} \\
5a^2+17c^2 \pm 4b & = & 17u^2 & 34u^2 \\
5a^2+17c^2 \mp 4b & = & v^2 & 2v^2 \\
a^2+5c^2 & = & uv & 2uv
\end{array}
$$

ここで，第 1 の可能性では

$$10a^2+34c^2 = 17u^2+v^2$$
$$a^2+5c^2 = uv$$

である．これが $\boldsymbol{Q}_{17}$ で不可能であることを示そう．$|\ \ | = |\ \ |_{17}$ と書く．斉次性から

$$\max(|a|, |c|, |u|, |v|) = 1\,.$$

10 は 17 の平方非剰余なので

$$|a| < 1, \quad |v| < 1$$

である．また 2 つめの方程式から

$$|c| < 1$$

である．最後に 1 つめの方程式から

$$|u| < 1$$

であるが，これは矛盾である．

また，第 2 の可能性では

$$5a^2+17c^2 = 17u^2+v^2$$
$$a^2+5c^2 = 2uv$$

を得る．これが $\boldsymbol{Q}_{17}$ で考えて不可能であることも第 1 の場合と同様に示すことができる． ∎

【演習問題】

1 ［数的整数論を用いよ.］ 定理 2 の別証を次の方針にしたがって与えよ．

（i） 体 $\boldsymbol{Q}(\sqrt{17})$ の類数は 1 であること，整数環の基底は $1, \dfrac{1}{2}(1+\sqrt{17})$ であること，およびノルムが -1 の基本単数は $4+\sqrt{17}$ であることを示せ．素

数 2 は $(5\pm\sqrt{17})/2$ に分解することを示せ．

（ii）
$$a^4-17c^4=2b^2$$

整数 a, b, c で $\gcd(a, c)=1$ とする．このとき，a, c は奇数で

$$\frac{a^2\pm c^2\sqrt{17}}{2}$$

は互いに素であることを示せ．

（iii）　適当な単数 η と適当な整数 μ をとれば

$$\frac{a^2+\sqrt{17}\,c^2}{2}=\left(\frac{5\pm\sqrt{17}}{2}\right)\eta\mu^2 \qquad (*)$$

となることを示せ．

（iv）　実数体への埋め込みのどちらをとっても，$\eta>0$ であることを示せ．これから η は平方数であり，したがって，μ^2 に含まれることを示せ．

（v）　$\eta=1$，$\mu=(u+v\sqrt{17})/2$ とおき，$\sqrt{17}$ と独立な項を等しいとおけば，$4a^2=5(u^2+17v^2)\pm34uv$ を得るが，これは $\boldsymbol{Q}_3$ で（$\boldsymbol{Q}_{17}$ でも）不可能であることを示せ．

19

ガロアコホモロジーの初歩

次章では $\overline{\boldsymbol{Q}}$ 上で双有理同値になるような $\boldsymbol{Q}$ 上定義された 2 つの曲線を取り扱うが，ここではまず簡単な例を考える．その後，一般的な仕組を解説しよう．

2 次曲線

$$\mathcal{A}:\ X_1^2+X_2^2=3$$

は有理点をもたないので，$\boldsymbol{Q}$ 上の直線に同型ではない．しかしながら，$\boldsymbol{Q}(\sqrt{3})$ では直線と次の対応で双有理同値である（y は直線の座標を表す）．

$$y=(x_1-\sqrt{3})/x_2$$

$$x_1=\frac{\sqrt{3}(1-y^2)}{y^2+1},\quad x_2=\frac{-2\sqrt{3}\,y}{y^2+1}.$$

ここで y が超越的ならば，(x_1, x_2) は $\mathcal{A}$ の生成点である．

ガロア群 $\mathrm{Gal}(\boldsymbol{Q}(\sqrt{3})/\boldsymbol{Q})$ の $\boldsymbol{Q}(\sqrt{3}, y)=\boldsymbol{Q}(\sqrt{3}, x_1, x_2)$ への作用は 2 通りのものが考えられる．つまり，y に自明に作用するか，(x_1, x_2) に自明に作用するかの 2 通りである．

最初の場合は，ガロア群の自明でない元は $\mathcal{A}$ の自己同型

$$x_1\to -x_1,\quad x_2\to -x_2$$

を引き起こす．2 番目の場合は，直線の自己同型

$$y\to -1/y$$

を引き起こす．この例では，2 つの関数体を同一視する $\boldsymbol{Q}(\sqrt{3})$ 上定義され

た双有理同型を用いた．一般的な状況でこのことを明確に定式化しておいた方がよい．

$\mathcal{A}, \mathcal{B}$ は $\boldsymbol{Q}$ 上定義された2つの曲線，

$$\phi: \ \mathcal{A} \to \mathcal{B}$$

は $\overline{\boldsymbol{Q}}$ 上定義された双有理同型とする．$\sigma \in \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ を ϕ の係数に作用させれば，もう1つの双有理同型

$$\sigma\phi: \ \mathcal{A} \to \mathcal{B}$$

を得る．すると，

$$\theta_\sigma := (\sigma\phi)\phi^{-1}: \ \mathcal{B} \to \mathcal{B}$$

は $\overline{\boldsymbol{Q}}$ 上定義された双有理自己同型である．$\tau \in \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ は θ_σ に作用し，

$$\begin{aligned} \tau\theta_\sigma &= (\tau\sigma\phi)(\tau\phi)^{-1} \\ &= [(\tau\sigma\phi)\phi^{-1}][\phi(\tau\phi)^{-1}] \\ &= \theta_{\tau\sigma}\theta_\tau^{-1} \end{aligned}$$

をみたす．ゆえに

$$\theta_{\tau\sigma} = (\tau\theta_\sigma)\theta_\tau$$

を得る．これは**コサイクル恒等式**[*1]であり，$\{\theta_\sigma\}$ は**コサイクル**であることがわかる．

他に $\overline{\boldsymbol{Q}}$ 上定義された双有理同型

$$\phi': \ \mathcal{A} \to \mathcal{B}$$

があったとしよう．すると，自己同型

$$\omega: \ \mathcal{B} \to \mathcal{B}$$

を適当に選んで，

$$\phi' = \omega\phi$$

とできる．すると，

$$\begin{aligned} \theta'_\sigma &= (\sigma\phi')(\phi'^{-1}) \\ &= \sigma\omega\theta_\sigma\omega^{-1} \end{aligned}$$

---

*1 このロココ風の言い回しはトポロジストによる．

が成り立つ.

このとき，2つのコサイクル $\{\theta_\sigma\}$, $\{\theta'_\sigma\}$ は**コホモローグ**という.

ϕ が $\boldsymbol{Q}$ 上定義されていれば

$$\theta'_\sigma = (\sigma\omega)\omega^{-1}$$

となり，これは**コバウンダリー**にほかならない．この場合，双有理同型をうまくとれば $\mathcal{A}$, $\mathcal{B}$ は $\boldsymbol{Q}$ 上の双有理同値になる.

$\mathcal{B}$ とコサイクル $\{\theta_\sigma\}$ が与えられたとき，（$\boldsymbol{Q}$ 上の双有理同値を除いて）$\mathcal{A}$ を再構成することができる．$\mathcal{B}$ の生成点 $\boldsymbol{x}$ に対して，$\sigma\in\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ の $\overline{\boldsymbol{Q}}(\boldsymbol{x})$ への作用 $\tilde{\sigma}$ を

$$\left.\begin{array}{c}\tilde{\sigma}\text{ は }\overline{\boldsymbol{Q}}\text{ 上には }\sigma\text{ として作用}\\ \tilde{\sigma}\boldsymbol{x}=\theta_\sigma\boldsymbol{x}\end{array}\right\}$$

と定める．すると $\tau\in\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ に対して

$$\begin{aligned}\tilde{\tau}(\tilde{\sigma}\boldsymbol{x}) &= (\tau\theta_\sigma)(\tilde{\tau}\boldsymbol{x})\\ &= (\tau\theta_\sigma)\theta_\tau\boldsymbol{x}\\ &= \theta_{\tau\sigma}\boldsymbol{x}\end{aligned}$$

が得られ，これから

$$(\widetilde{\tau\sigma}) = \tilde{\tau}\tilde{\sigma}$$

であることがわかる.

$\tilde{\sigma}$ の不変体は $\boldsymbol{Q}$ 上の双有理同値を除いて $\mathcal{A}$ を与える.

【演習問題】

1　σ が $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ 上のすべての元を動くとき，直線を2次曲線

$$X_1^2+X_2^2=n$$

に“ねじる”直線の双有理自己同型のコサイクル $\{\theta_\sigma\}$ を求めよ．ここで n は $\boldsymbol{Q}^*$ の任意の元とする.

$n=5$ のとき，求めたコサイクルがコバウンダリーであることを直接計算によって示せ.

$n=3$ のときはコバウンダリーになっているか.

20

ヤコビ多様体の構成

$\mathcal{D}$ は $\boldsymbol{Q}$ 上定義された種数 1 の曲線とする．この章では，曲線 $\mathcal{D}$ と密接に関連した楕円曲線 $\mathcal{C}$ で $\boldsymbol{Q}$ 上定義されるものを構成しよう．それらの関係は次章以降で次第に明らかになる．

最初にまず楕円曲線の間の双有理同型を考察しよう．まず一般の体上で考える．2 つの楕円曲線

$$\mathcal{C}_j:\ Y^2 = X^3 + A_jX + B_j \qquad (j = 1, 2)$$

に対して

$$\phi:\ \mathcal{C}_1 \to \mathcal{C}_2$$

を双有理同型とする．$\phi(\boldsymbol{x})$ のかわりに $\phi(\boldsymbol{x}) - \phi(\boldsymbol{o}_1)$ を考えて

$$\phi(\boldsymbol{o}_1) = \boldsymbol{o}_2$$

と仮定しても一般性を失わないことがわかる．ここで $\boldsymbol{o}_j$ は $\mathcal{C}_j$ の無限遠点である．

この双有理同型は位数 1 の極をもつ関数を同じ型の関数にうつす．したがって，a, b を適当に選べば

$$\phi(X) = aX + b$$

と書ける．同様に，

$$\phi(Y) = cY + dX + e$$

と書けることがわかる．$\mathcal{C}_j$ の方程式の形から

$$d = e = 0, \quad b = 0, \quad a^3 = c^2$$

であり，したがって，適当に s をとれば

$$a=s^2, \quad c=s^3$$

と書けることがわかる．これより，

$$A_2=s^4A_1, \quad B_2=s^6B_1 \tag{1}$$

を得る．

特に $A_1^3/B_1^2=A_2^3/B_2^2$ は双有理同値で不変である．

楕円曲線

$$\mathcal{C}:\ Y^2=X^3+AX+B$$

の双有理不変量としては

$$j=j(\mathcal{C})=\frac{1728(4A^3)}{4A^3+27B^2}$$

を考えるのが通例である．この不変量に関しては通常 j という記号を用いる．定数 $1728=12^3$ は複素関数論に由来するものである．すべての楕円曲線に対して j は有限な値をとることに注意する．j が無限になるのは楕円曲線が退化したときである．

補題 1　双有理同値である 2 つの楕円曲線は s を適当にとれば，(1)の関係が成り立つ．特にこれらの楕円曲線の j 不変量は一致する．さらにこの s は曲線および双有理同型が定義される体の元である． □

系　楕円曲線

$$\mathcal{C}:\ Y^2=X^3+AX+B$$

の $\boldsymbol{o}$ を $\boldsymbol{o}$ にうつす任意の双有理同型は

$$Y\to s^3Y, \quad X\to s^2X$$

の形にとれる．もし，$AB\neq 0$ であれば $s^2=1$ である．$B=0$ であれば，$s^4=1$ であり，$A=0$ であれば $s^6=1$ である．

［証明］ (1)で $\mathcal{C}=\mathcal{C}_1=\mathcal{C}_2$ とおけば明らか． ▮

この章の本題にもどろう．$\mathcal{D}$ は $\boldsymbol{Q}$ 上定義された種数 1 の曲線とする．一般的には $\mathcal{D}$ 上に有理点は存在しないし，また存在したとしてもそれを求めることはできないかもしれない．しかし $\overline{\boldsymbol{Q}}$ 上定義される $\mathcal{D}$ の点を見いだすのは容易である．したがって $\overline{\boldsymbol{Q}}$ 上定義された双有理同型

$$\phi:\ \mathcal{D} \to \mathcal{C}$$

が存在する．ここで $\mathcal{C}$ は $\overline{\boldsymbol{Q}}$ 上定義された $\mathcal{D}$ の標準形(楕円曲線)である．

元 $\sigma \in \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ は双有理同型 ϕ に作用し，

$$\sigma\phi:\ \mathcal{D} \to \sigma\mathcal{C}$$

なる双有理同型を得る．ここで

$$\sigma\mathcal{C}:\ Y^2 = X^3 + \sigma A X + \sigma B$$

である．

したがって，$\mathcal{C}$ と $\sigma\mathcal{C}$ とは $\overline{\boldsymbol{Q}}$ 上 $(\sigma\phi)\phi^{-1}$ によって双有理同型である．ゆえに

$$\sigma j(\mathcal{C}) = j(\sigma\mathcal{C}) = j(\mathcal{C})$$

が成り立つ．(σ は $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ の任意の元であるから) $j(\mathcal{C}) \in \boldsymbol{Q}$ である．$AB \neq 0$ であれば，これは $A^3/B^2 \in \boldsymbol{Q}$ を意味する．そこで変換 $X \to t^2 X,\ Y \to t^3 Y\ (t \in \overline{\boldsymbol{Q}})$ を適当にとって $\mathcal{C}$ は $\boldsymbol{Q}$ 上定義されていると仮定しても一般性を失わないことがわかる．

もちろん，一般には ϕ は $\overline{\boldsymbol{Q}}$ 上で定義されているだけである．ところで

$$\theta_\sigma = (\sigma\phi)\phi^{-1}$$

は $\mathcal{C}$ の自己同型である．

まず

$$AB \neq 0$$

と仮定しよう．補題 1 と系より $\mathcal{C}$ の自己同型 θ_σ は

$$\theta_\sigma:\ \boldsymbol{x} \to \varepsilon_\sigma \boldsymbol{x} + \boldsymbol{a}_\sigma$$

と書けることがわかる．ここで $\boldsymbol{a}_\sigma$ は $\overline{\boldsymbol{Q}}$ 上定義された点であり，$\varepsilon_\sigma = \pm 1$ である(訳者注．θ_σ は無限遠点を無限遠点にうつさない可能性があるので $\boldsymbol{a}_\sigma$ が必要)．ここで前章で述べたことを用いれば，

$$\theta_{\tau\sigma} = (\tau\theta_\sigma)\theta_\tau$$

が成り立つ．特に，$\varepsilon_\sigma \in \boldsymbol{Q}$ であるので

$$\varepsilon_{\tau\sigma} = \varepsilon_\sigma \varepsilon_\tau$$

が成り立ち，ε_σ は群指標であることがわかる．

ε_σ は常に 1 にとれることを示そう．もし $\varepsilon_\sigma \neq 1$ なる σ があるとすると，

$$\sigma(\sqrt{d}) = \varepsilon_\sigma \sqrt{d} \qquad (\sigma \in \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q}))$$

が成り立つような $d \in \boldsymbol{Q}$ が存在する．変換

$$X \to dX, \quad Y \to d\sqrt{d}Y$$

によって $\boldsymbol{Q}$ 上定義された新しい楕円曲線 $\mathcal{C}$ が得られ，この楕円曲線に対しては常に $\varepsilon_\sigma = 1$ である．

$AB=0$ のときも同様の結論を得るが，もう少し深い議論が必要である*1．$B=0$ としよう．したがって，$\varepsilon_\sigma^4 = 1$ である．ここで，

$$\boldsymbol{x} \to \varepsilon \boldsymbol{x}$$

は

$$X \to \varepsilon^2 X, \quad Y \to \varepsilon Y$$

で定義した．さて，$\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ は ε に作用して

$$\varepsilon_{\tau\sigma} = (\tau \varepsilon_\sigma)\varepsilon_\tau$$

である．Hilbert の定理 90（演習問題参照）から，$\delta^4 \in \boldsymbol{Q}$ かつ

$$\sigma\delta = \varepsilon_\sigma \delta$$

をみたす $\delta \in \overline{\boldsymbol{Q}}$ が存在する．この δ を用いて，上のように座標変換を行なって新しい曲線 $\mathcal{C}$ を構成すると $\varepsilon_\sigma = 1$ であることがわかる．$A=0$ のときも同様である．

このようにして，どの場合も $\boldsymbol{Q}$ 上定義された楕円曲線 $\mathcal{C}$ と $\overline{\boldsymbol{Q}}$ 上定義された双有理同型

$$\phi: \ \mathcal{D} \to \mathcal{C}$$

で，すべての $\sigma \in \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ に対して

$$(\sigma\phi)\phi^{-1} = \theta_\sigma: \ \boldsymbol{x} \to \boldsymbol{x} + \boldsymbol{a}_\sigma$$

が成り立つものが存在することがわかる．

以上をまとめて次の定理が証明できた．

定理 1　$\mathcal{D}$ は $\boldsymbol{Q}$ 上定義された種数 1 の曲線とする．このとき以下の条件をみたす $\boldsymbol{Q}$ 上定義された楕円曲線 $\mathcal{C}$ と，$\overline{\boldsymbol{Q}}$ 上定義された双有理同型が存在する：

---

*1　したがって，最初に読むときはとばしてもよい．

$$\phi:\ \mathcal{D} \to \mathcal{C}$$

で，任意の $\sigma \in \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ に対して写像

$$\theta_\sigma = (\sigma\phi)\phi^{-1}:\ \mathcal{C} \to \mathcal{C}$$

が適当な $\overline{\mathfrak{G}}$ の元 $\boldsymbol{a}_\sigma$ を用いて

$$\theta_\sigma:\ \boldsymbol{x} \to \boldsymbol{x} + \boldsymbol{a}_\sigma$$

と書ける．

さらに，$\mathcal{C}$ は $\boldsymbol{Q}$ 上の双有理同値を除いて一意的に定まる．　□

この楕円曲線 $\mathcal{C}$ を $\mathcal{D}$ の**ヤコビ多様体**とよぶ．これらのことをさらに調べるためには次章で導入する新しい手法が必要となる．

【演習問題】

1　以下の楕円曲線のヤコビ多様体を構成せよ．

（i）　$Y^2 = aX^4 + bX^2 + c \qquad (a,\ c \in \boldsymbol{Q}^*,\ b \in \boldsymbol{Q},\ b^2 - 4ac \neq 0)$

（ii）　$aX^3 + bY^3 + cZ^3 = 0 \qquad (a,\ b,\ c \in \boldsymbol{Q}^*)$

（iii）　$aX^3 + bY^3 + cZ^3 + mXYZ = 0 \qquad (a,\ b,\ c,\ m \in \boldsymbol{Q}^*)$

（iv）　$Y^2 = aX^4 + bX^3 + cX^2 + dX + e$

2　$\mathcal{D}$ は次の方程式系で定義される種数 1 の曲線とする．

$$\begin{aligned}(e_2 - e_1)t^2 &= d_1 v_1^2 - d_2 v_2^2 \\ (e_3 - e_2)t^2 &= d_2 v_2^2 - d_3 v_3^2 \\ (e_1 - e_3)t^2 &= d_3 v_3^2 - d_1 v_1^2\end{aligned}$$

ここで e_1, e_2, e_3 は相異なり，$d_j \in \boldsymbol{Q}^*$，$d_1 d_2 d_3 = 1$ とする．$\kappa = \boldsymbol{Q}(d_1^{1/2},\ d_2^{1/2})$ 上で定義された $\mathcal{D}$ の点があり，これを用いて，κ 上定義された写像

$$\phi:\ \mathcal{D} \to \mathcal{C},$$

ここで

$$\mathcal{C}:\ Y^2 = (X - e_1)(X - e_2)(X - e_3)$$

が存在することを示せ．コサイクル

$$(\sigma\phi)\phi^{-1} = \theta_\sigma:\ \mathcal{C} \to \mathcal{C}, \quad \sigma \in \mathrm{Gal}(\kappa/\boldsymbol{Q})$$

は

$$\boldsymbol{x} \to \boldsymbol{x} + \boldsymbol{a}_\sigma \qquad \text{ただし } 2\boldsymbol{a}_\sigma = \boldsymbol{o}$$

の形をしていることを示せ．これから $\mathcal{C}$ は $\mathcal{D}$ のヤコビ多様体であることを導け．

3　この問題では基礎体は $\boldsymbol{Q}(\rho)$, $\rho^3=1$, $\rho \neq 1$ とする．$\boldsymbol{Q}(\rho)$ の元 a, b, c に対して曲線

$$\mathcal{D}:\ aU^3+bV^3+cW^3=0$$
$$\mathcal{C}:\ X^3+Y^3+abcZ^3=0$$

を考える．$\kappa=\boldsymbol{Q}(\rho, a^{1/3}, b^{1/3})$ とおき，

$$X=a^{1/3}U, \quad Y=b^{1/3}V, \quad Z=a^{-1/3}b^{-1/3}W$$

で決まる写像 ϕ: $\mathcal{D} \to \mathcal{C}$ を考える．この ϕ に対応する θ_σ は

$$\theta_\sigma:\ \boldsymbol{x} \to \boldsymbol{x}, \quad \text{または} \quad \boldsymbol{x}+(\rho, -\rho^2, 0), \quad \text{または} \quad \boldsymbol{x}+(\rho^2, -\rho, 0)$$

であることを示せ．これから $\mathcal{C}$ は $\mathcal{D}$ のヤコビ多様体であることを導け．

残りの演習問題は（本文の記号を用いると），$AB=0$ のとき $\varepsilon_\sigma=1$ とできることの証明を補うものである．

4　κ/k は n 次の有限次正規（分離）拡大とする．$\alpha_1, \cdots, \alpha_n$ を κ/k の基底，$\sigma_1, \cdots, \sigma_n$ はガロア群の元とする．

$$\det[\sigma_i \alpha_j] \neq 0$$

であることを示せ．

［ヒント．適当な β をとれば $\kappa=k(\beta)$ とできる．

注意．今なお，ガロア理論のもっとも優れた入門書の 1 つ *Galois Theory*, Notre Dame Mathematical Lectures **2**, 1942, 2nd ed. 1948,（邦訳）寺田文行（訳），ガロア理論入門，東京図書，1974 で，E. Artin はこの事実を帰納法を用いて証明している．］

5　κ/k は有限次正規（分離）拡大とする．$\sigma \in \mathrm{Gal}(\kappa/k)$ に対して $\theta_\sigma \in k^*$ はコサイクル条件

$$\theta_{\tau\sigma}=(\tau\theta_\sigma)\theta_\tau$$

を満足するように与えられているとする．$\{\theta_\sigma\}$ はコバウンダリーであることを示せ．すなわち，すべての $\sigma \in \mathrm{Gal}(\kappa/k)$ に対して

$$\theta_\sigma=(\sigma\gamma)\gamma^{-1}$$

をみたす $\gamma \in \kappa^*$ が存在する．

［ヒント．$\lambda \in \kappa$ に対して

$$\gamma=\sum_\sigma \theta_\sigma(\sigma\lambda)$$

は$\gamma \neq 0$であれば求めるものであることを示せ．補題2を用いてλが$\gamma \neq 0$であるようにとれることを示せ．

注意．この結果はヒルベルトの数論報告──前世紀末にドイツ数学会に提出した代数的整数論に関する報告──の定理90にあたるので通常Hilbertの定理90（またはSatzの定理90）という名で使われる．]

6　nを1より大きい整数とする．$\sigma \in \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$に対して$\theta_\sigma$は1の$n$乗根であり，かつ$\{\theta_\sigma\}$はコサイクルとせよ．このとき元$\delta \in \overline{\boldsymbol{Q}}$で

$$\theta_\sigma = (\sigma\delta)\delta^{-1}, \quad \delta^n \in \boldsymbol{Q}$$

なるものが存在することを示せ．

21

抽象論からの準備 [*1]

有限群 Γ はアーベル群 A（算法は加法的に表す）に作用しているとし，作用は σA $(\sigma \in \Gamma,\ a \in A)$ と表す．

群 Γ の**コサイクル**とは写像 $\Gamma \to A$ であって，それを

$$\sigma \to a_\sigma$$

と表すとき，**コサイクル恒等式**

$$\tau a_\sigma = a_{\tau\sigma} - a_\tau \qquad (\sigma,\ \tau \in \Gamma)$$

をみたすものをいう．$\tau = 1$（Γ の単位元）に対しては，この条件から

$$a_1 = 0$$

が導かれる．

$b \in A$ に対して

$$a_\sigma = \sigma b - b$$

とおいて Γ から A への写像を定義すれば，これがコサイクルであることが容易にわかる．この種のコサイクルを**コバウンダリー**とよぶ．

コサイクルは各成分ごとの和

$$\{a_\sigma\} + \{b_\sigma\} = \{a_\sigma + b_\sigma\}$$

---

*1　この章は群のコホモロジー論と可換なガロアコホモロジー論から必要な部分だけを過不足なくまとめたものである．詳しくは，例えば，J. W. S. Cassels and A. Fröhlich (eds.): *Algebraic number theory*, Academic Press, 1967 を参照．ここでの取り扱いは C. Chevalley: *Class field theory*, Nagoya, 1954 で示唆されているものである．

により群になる．コバウンダリーはこの群の部分群である．商群は**1次元コホモロジー群**

$$H^1(\Gamma, A)$$

である．

さて，Γ はいろいろなもの(群構造の転移したもの)に作用する．Γ は自分自身に内部自己同型として作用する．したがって，τ は写像(コサイクル)

$$\{a_\sigma\}:\ \sigma \to a_\sigma$$

に

$$\begin{aligned}\tau\{a_\sigma\}:\ \tau\sigma\tau^{-1} &\to \tau a_\sigma \\ &= a_{\tau\sigma} - a_\tau\end{aligned}$$

と作用する．$\tau\sigma\tau^{-1}$ を σ と書き直すと

$$\tau\{a_\sigma\}:\ \sigma \to a_{\sigma\tau} - a_\tau$$

となる．これは当然期待されるようにコサイクルである．実際，

$$\begin{aligned}\tau\{a_\sigma\} - \{a_\sigma\}:\ \sigma &\to a_{\sigma\tau} - a_\tau - a_\sigma \\ &= \sigma a_\tau - a_\tau\end{aligned}$$

となり，コバウンダリーであることがわかる．したがって，次の補題を得る．

補題 0　Γ は $H^1(\Gamma, A)$ に自明に作用する．　□

補題 1　$H^1(\Gamma, A)$ のすべての元は有限位数であり，かつその位数は $\sharp\Gamma$ を割り切る*2．

［証明］　$H^1(\Gamma, A)$ の元がコサイクル $\{a_\sigma\}$ で代表されたとする．上の補題によりこの元はコサイクル

$$\tau\{a_\sigma\} = \{a_{\sigma\tau} - a_\tau\}$$

でも代表される．一方，

$$\sum_\tau \tau\{a_\sigma\} = \{0\}$$

である．[$a_1 = 0$ に注意.]　▮

補題 2　$m \in \boldsymbol{Z}$, $m > 1$ に対して A の元で位数が m の約数であるもの全体

---

*2　$\sharp\Gamma$ は Γ の元の個数すなわち，群 Γ の位数を表す．

を $\Delta_m \subset A$ と記す．A の元はすべて A 内で m で割り切れる（すなわち，$a \in A$ に対して $mb=a$ をみたす $b \in A$ が存在する）と仮定する．

このとき，$H^1(\Gamma, A)$ の位数 m の元はコサイクル $\{d_\sigma\}$, $d_\sigma \in \Delta_m$ で代表される．

［証明］ $H^1(\Gamma, A)$ の位数 m の元がコサイクル $\{a_\sigma\}$ で代表されたとする．仮定から $m\{a_\sigma\}$ はコバウンダリーであり，

$$ma_\sigma = \sigma b - b \qquad (b \in A)$$

と書ける．補題の仮定より，$b=mc$, $c \in A$ と書けるので，

$$ma_\sigma = m\sigma c - mc$$

と書ける．すなわち，

$$m(a_\sigma - \sigma c + c) = 0$$

が成り立つ．したがって $H^1(\Gamma, A)$ の元は コサイクル

$$\sigma \to a_\sigma - \sigma c + c \in \Delta_m$$

で代表され，補題が示された． ∎

Γ で固定される A の元を A^Γ と記す．つまり，

$$a \in A^\Gamma \quad \Leftrightarrow \quad \sigma a = a \qquad (すべての\,\sigma \in \Gamma)$$

である．

補題 3　記号と仮定は前の補題と同じとする．

$$A^\Gamma / mA^\Gamma$$

は $H^1(\Gamma, \Delta_m)$ の部分群と標準的に同型である．

［証明］ 仮定より $a \in A^\Gamma$ に対して

$$a = mb, \qquad b \in A$$

が成り立つ．$\sigma \in \Gamma$ を作用させることにより，

$$a = \sigma a = m\sigma b$$

であるから

$$md_\sigma = 0, \quad d_\sigma = \sigma b - b$$

を得る．$\{d_\sigma\}$ は Δ_m に値をとるコサイクルである（$\{d_\sigma\}$ は A ではコバウンダリーになっているが，Δ_m ではコバウンダリーとは限らない）．

a が与えられたとき，上の b のとり方は一意的ではないがどのようなと

り方をしても $b+c$, $c\in\Delta_m$ の形をしている．したがって，$\{d_\sigma\}$ で定まる $H^1(\Gamma, \Delta_m)$ の元は a から一意的に定まる．

もし $a\in mA^\Gamma$ であれば，$b\in A^\Gamma$ にとれるので，すべての σ に対して $d_\sigma=0$ となり，$H^1(\Gamma, \Delta_m)$ での像は 0 となる．

逆に上のように構成されたコサイクルがコバウンダリーである，すなわち，任意の $\sigma\in\Gamma$ に対して

$$d_\sigma = \sigma e - e$$

をみたす Δ_m の元 e が存在したとする．すると，すべての $\sigma\in\Gamma$ に対して

$$\sigma(b-e) = b-e$$

であり，

$$b-e\in A^\Gamma, \quad m(b-e) = a$$

となる． ∎

以上 2 つの補題はまとめることができる．仮定も繰り返して書いておく．

定理　A のすべての元は正整数 $m>1$ で割り切れるとする（すなわち，任意の元 a に対して $mb=a$ をみたす $b\in A$ が存在する）．このとき

$$0\to A^\Gamma/mA^\Gamma \to H^1(\Gamma, \Delta_m)\to[H^1(\Gamma, A)]_m\to 0$$

は完全列である．ここで $[\cdots]_m$ は位数が m の約数であるような元全体からなる部分群であり，3 番目の写像は $\Delta_m\hookrightarrow A$ より引き起こされるものである．

［証明］　補題 2, 3 により，$H^1(\Gamma, \Delta_m)$ での完全性，すなわち，

$$A^\Gamma/mA^\Gamma \to H^1(\Gamma, \Delta_m)$$

の像が

$$H^1(\Gamma, \Delta_m)\to[H^1(\Gamma, A)]_m$$

の核とちょうど一致することを示すだけでよい．

コサイクル $\{d_\sigma\}$ で与えられる最初の写像の像に含まれる元を考えよう．仮定より $d_\sigma=\sigma b-b$, $b\in A$ なので，$\{d_\sigma\}$ を A に値をとるコサイクルと考えるとコバウンダリーである．したがって (像 ⊂ 核) である．

次に $\{d_\sigma\}$ で代表される $H^1(\Gamma, \Delta_m)$ の元が核に属している，すなわち，$\{d_\sigma\}$ は A でのコバウンダリーで，ある $b\in A$ によって $d_\sigma=\sigma b-b$ と書けたとする．すると，すべての $\sigma\in\Gamma$ に対して

$$\sigma(mb)-mb = md_\sigma = 0$$

となり，$mb \in A^\Gamma$ である．よって，$\{d_\sigma\}$，$d_\sigma = \sigma b - b$ は $a = mb \in A^\Gamma$ より定まる $H^1(\Gamma, \Delta_m)$ の元の代表となり，(核⊂像) である． ▮

ガロアコホモロジー　体 k に対して $\overline{k}$ をその分離閉包(標数 0 の場合は代数閉包と一致する)とする．

$$\Gamma = \mathrm{Gal}(\overline{k}/k)$$

とおく．群 Γ のアーベル群 A への作用 $a \to \sigma a$ $(\sigma \in \Gamma,\ a \in A)$ が次の条件をみたすとき，この作用は**連続**であるという．

任意の $a \in A$ に対して k の有限次拡大 κ，$[\kappa : k] < \infty$ (この拡大体は a によって変わってよい)があり，すべての $\sigma \in \mathrm{Gal}(\overline{k}/\kappa) \subset \mathrm{Gal}(\overline{k}/k)$ に対して

$$\sigma a = a$$

が成り立つ． □

注意 1　$k = \boldsymbol{Q}$，$\mathcal{C} : \boldsymbol{Q}$ 上定義された曲線，$Y^2 = X^3 + AX + B$，$A = \overline{\mathfrak{G}}$ がその 1 例である．

注意 2　A に自然な位相が入っていてもそれは無視する．“連続” という言葉はここでは単に技術的な用語にすぎない．通常の意味では，ここでの連続とは，Γ には適当な位相が入り，A には**離散位相**を入れて考えた場合に対応する．

以下の条件を満足する写像

$$\sigma \to a_\sigma \qquad (\sigma \in \Gamma,\ a_\sigma \in A)$$

を**連続なコサイクル**という．

(i)　コサイクル条件

$$\tau a_\sigma = a_{\tau\sigma} - a_\tau \qquad (\sigma, \tau \in \Gamma)$$

をみたす．

(ii)　有限次正規拡大 κ/k，$[\kappa : k] < \infty$ で，a_σ が κ 上の σ の作用のみに依存するものがあるという意味で連続である(もちろん，κ は $\{a_\sigma\}$ によってもよい)．

特に，すべての $\tau \in \mathrm{Gal}(\overline{k}/\kappa)$ に対して

$$a_\tau = 0$$

であり，すべての $\tau \in \mathrm{Gal}(\overline{k}/\kappa)$ に対して

$$\tau a_\sigma = a_{\tau\sigma} - a_\tau = a_\sigma - 0$$

が成り立ち，任意の $\sigma \in \mathrm{Gal}(\bar{k}/\kappa)$ に対して

$$a_\sigma \in A^{\mathrm{Gal}(\bar{k}/\kappa)}$$

である．

もし $\{a_\sigma\}$, $\{b_\sigma\}$ が連続なコサイクルであれば，$\{a_\sigma + b_\sigma\}$ も連続である．

コバウンダリー $\{\sigma c - c\}$, $c \in A$ は，Γ が A に連続的に作用するという仮定により，自動的に連続である．

定義　$H^1(\Gamma, A)$ は連続なコサイクル全体のコバウンダリーによる剰余群である． □

Γ が有限群の場合の証明から，以下の結果はただちに導くことができる．

定理 1　$H^1(\Gamma, A)$ はねじれ群である(すなわち，すべての元は有限位数である)． □

定理 2　正整数 $m > 1$ に対して A の各元は m で割り切れるとする．このとき，

$$0 \to A^\Gamma/mA^\Gamma \to H^1(\Gamma, \Delta_m) \to [H^1(\Gamma, A)]_m \to 0$$

は完全列である．ここで(前と同様に)

(i)　A^Γ は Γ で固定される元 $a \in A$ のなす集合であり，

(ii)　Δ_m は位数が m の約数であるような A の元からなる集合であり，

(iii)　$[H^1(\Gamma, A)]_m$ は位数が m の約数であるような $H^1(\Gamma, A)$ の元からなる集合である． □

付録 *3．局所化

素数 p を固定し，埋め込み

$$\lambda: \ \overline{\boldsymbol{Q}} \hookrightarrow \overline{\boldsymbol{Q}}_p$$

を 1 つ選ぶ．

---

*3　最初に読むときはとばしてよい．後に述べるようにここで得られる結果はこの本の別の観点からは自明なことである．

$$\Gamma = \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q}),$$
$$\Gamma_p = \mathrm{Gal}(\overline{\boldsymbol{Q}}_p/\boldsymbol{Q}_p)$$

と記すと λ は埋め込み

$$\lambda^*:\ \Gamma_p \hookrightarrow \Gamma$$

を引き起こす.

A が連続な Γ–加群とすると，λ^* によって A は連続な Γ_p–加群となる.

連続なコサイクル $\{a_\sigma\}$, $\sigma \in \Gamma$ に対して，σ を Γ_p に制限することによって連続な Γ_p コサイクルができる．したがって群の準同型

$$\lambda I:\ H^1(\Gamma, A) \to H^1(\Gamma_p, A)$$

ができる[**局所化**：“制限写像” の特別な場合にほかならない].

表面上は λI は埋め込み λ によっているが，実はそうでないことが示される.

任意の埋め込み Λ: $\overline{\boldsymbol{Q}} \hookrightarrow \overline{\boldsymbol{Q}}_p$ は $\overline{\boldsymbol{Q}}/\boldsymbol{Q}$ の自己同型 μ を適当に選ぶと

$$\Lambda = \lambda\mu$$

と書くことができる．有限群 Γ を論じた部分の補題 0 の類似により，μ は $H^1(\Gamma, A)$ に自明に作用する．したがって，$\Lambda I = \lambda I$ となる．こうして写像

$$H^1(\Gamma, A) \to H^1(\Gamma_p, A)$$

は，埋め込み $\overline{\boldsymbol{Q}} \hookrightarrow \overline{\boldsymbol{Q}}_p$ によらずに標準的であることがわかる.

この本では上述の議論は以下のように使われる．$\boldsymbol{Q}$ 上定義された楕円曲線

$$Y^2 = X^3 + AX + B$$

に対して，$\overline{\mathfrak{G}}, \overline{\mathfrak{G}}_p$ をこの楕円曲線のそれぞれ，$\overline{\boldsymbol{Q}}$ 上，$\overline{\boldsymbol{Q}}_p$ 上定義されている点の全体とする．問題とする写像

$$H^1(\Gamma, \overline{\mathfrak{G}}) \to H^1(\Gamma_p, \overline{\mathfrak{G}}_p)$$

であるが，この写像は写像の合成

$$H^1(\Gamma, \overline{\mathfrak{G}}) \to H^1(\Gamma_p, \overline{\mathfrak{G}}) \to H^1(\Gamma_p, \overline{\mathfrak{G}}_p)$$

とみなすことができる．ここで 2 番目の写像は埋め込み

$$\overline{\mathfrak{G}} \hookrightarrow \overline{\mathfrak{G}}_p$$

から引き起こされる.

後で，$H^1(\Gamma, \overline{\mathfrak{G}})$ の元は，$\boldsymbol{Q}$ 上定義された曲線 $\mathcal{D}$ とその上の主等質空間としての構造を 1 つ選んだものと解釈される．

$\boldsymbol{Q}$ 上定義された曲線 $\mathcal{D}$ は，その主等質空間としての構造と共に確かに $\boldsymbol{Q}_p$ 上でも定義されており，したがって $H^1(\Gamma_p, \overline{\mathfrak{G}}_p)$ のある元に対応する．こうして得られる写像 $H^1(\Gamma, \overline{\mathfrak{G}}) \to H^1(\Gamma_p, \overline{\mathfrak{G}}_p)$ が上で構成された写像そのものである．

22

主等質空間とガロアコホモロジー

第 20 章では $\boldsymbol{Q}$ 上定義された種数 1 の曲線 $\mathcal{D}$ に対して $\boldsymbol{Q}$ 上定義された楕円曲線

$$\mathcal{C}:\ Y^2 = X^3 + AX + B$$

と $\overline{\boldsymbol{Q}}$ 上定義された双有理同型

$$\phi:\ \mathcal{D} \to \mathcal{C}$$

が存在することを示した(第 20 章定理 1)．さらに，任意の $\sigma \in \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ に対して写像

$$(\sigma\phi)\phi^{-1}:\ \mathcal{C} \to \mathcal{C}$$

は

$$\boldsymbol{x} \to \boldsymbol{x} + \boldsymbol{a}_\sigma$$

と表すことができる．ここで $\boldsymbol{a}_\sigma \in \overline{\mathfrak{G}}$ である．

楕円曲線 $\mathcal{C}$ は変換

$$X \to s^2X, \quad Y \to s^3Y, \qquad s \in \boldsymbol{Q}^*$$

を法として一意的である．もちろん ϕ と $\boldsymbol{a}_\sigma$ は一意的には定まらない．楕円曲線 $\mathcal{C}$ は $\mathcal{D}$ の**ヤコビ多様体**とよばれるものであった．

これらの元 ϕ，$\boldsymbol{a}_\sigma$ がどれくらい自由に選ぶことができるのか論じる必要がある．(前説の議論から) $\boldsymbol{a}_\sigma$ はコサイクル恒等式

$$\tau\boldsymbol{a}_\sigma = \boldsymbol{a}_{\tau\sigma} - \boldsymbol{a}_\tau$$

をみたすことにまず注意する．$\boldsymbol{a}_\sigma$ は**可換群** $\overline{\mathfrak{G}}$ の元であり，第 21 章の手法を

使うことができる.

写像

$$\psi:\ \mathcal{C} \to \mathcal{C},\quad \boldsymbol{x} \to \boldsymbol{x}+\boldsymbol{b}\quad (\boldsymbol{b} \in \overline{\mathfrak{G}})$$

を使って，写像 ϕ を写像 $\phi\psi$ におきかえることにより，$\{\boldsymbol{a}_\sigma\}$ は

$$\boldsymbol{a}_\sigma + (\sigma\boldsymbol{b} - \boldsymbol{b})$$

に変わる．$\sigma\boldsymbol{b}-\boldsymbol{b}$ はコバウンダリーであり，可換な場合はコバウンダリー全体はコサイクル全体の部分群である．したがって，$\{\boldsymbol{a}_\tau\}$ は商群—$\Gamma = \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ の 1 次元コホモロジー群

$$\{コサイクル\}/\{コバウンダリー\} = H^1(\Gamma, \overline{\mathfrak{G}})$$

の元を定める.

第一歩として，楕円曲線 $\mathcal{C}$ から曲線 $\mathcal{D}$ と双有理同型 ϕ を構成できることを示そう．$\mathcal{C}$ の生成点 $\boldsymbol{x}$ に対して，$\sigma \in \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ の $\overline{\boldsymbol{Q}}(\boldsymbol{x})$ への作用 $\tilde{\sigma}$ が

（i） $\tilde{\sigma}$ は σ と同様に $\overline{\boldsymbol{Q}}$ 上に作用する

（ii） $\tilde{\sigma}\boldsymbol{x} = \boldsymbol{x} + \boldsymbol{a}_\sigma$

で与えられることに注意する．すると，この作用で固定される体は $\boldsymbol{Q}$ 上定義された曲線 $\mathcal{D}$ の関数体であり，$\overline{\boldsymbol{Q}}$ 上定義された ϕ は $\overline{\boldsymbol{Q}}$ 上での $\mathcal{C}$ と $\mathcal{D}$ との関数体の同型を与える.

写像 ϕ は次の意味で $\mathcal{D}$ に $\mathcal{C}$ 上の**主等質空間**の構造を与える.

$\mathcal{D}$ 上の独立な 2 つの生成点 $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2$ をとる．これらは $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ で固定されているとする.

$$\Delta(\boldsymbol{\xi}_1, \boldsymbol{\xi}_2) = \phi(\boldsymbol{\xi}_1) - \phi(\boldsymbol{\xi}_2)$$

とおくと

$$\begin{aligned}\sigma\Delta(\boldsymbol{\xi}_1, \boldsymbol{\xi}_2) &= (\phi(\boldsymbol{\xi}_1) + \boldsymbol{a}_\sigma) - (\phi(\boldsymbol{\xi}_2) + \boldsymbol{a}_\sigma)\\ &= \Delta(\boldsymbol{\xi}_1, \boldsymbol{\xi}_2)\end{aligned}$$

が成り立つ．すなわち，Δ で与えられる $\mathcal{D}$ 自身の 2 つの直積から $\mathcal{C}$ への代数的写像は $\boldsymbol{Q}$ 上定義されている．明らかに,

$$\Delta(\boldsymbol{\xi}_1, \boldsymbol{\xi}_2) + \Delta(\boldsymbol{\xi}_2, \boldsymbol{\xi}_3) = \Delta(\boldsymbol{\xi}_1, \boldsymbol{\xi}_3)$$

が成り立つ.

したがって，コサイクル $\{\boldsymbol{a}_\sigma\}$ あるいは $\{\boldsymbol{a}_\sigma\}$ に対応する $H^1(\Gamma, \overline{\mathfrak{G}})$ の元は

ペア $(\mathcal{D}, \Delta)$ を定める．コサイクル $\{-\boldsymbol{a}_\sigma\}$ はペア $(\mathcal{D}, -\Delta)$ を定める．このように群構造を考えるためには，曲線 $\mathcal{D}$ と共にヤコビ多様体だけでなくペア $(\mathcal{D}, \Delta)$ を考える必要がある．ここで Δ は主等質空間の構造を与える．

上の説明では 1 つだけ微妙な点を見過ごしている．$H^1(\Gamma, \overline{\mathfrak{G}})$ の元は $\mathcal{D}$ の関数体を定め，したがって曲線 $\mathcal{D}$ は $\boldsymbol{Q}$ 上定義された双有理同値を除いてしか定まらない．$\boldsymbol{Q}$ 上定義された $\mathcal{D}$ の自己同型が Δ を $-\Delta$ に変えることがおこりうる(!)．自明な例は $\mathcal{C}$ をそれ自身ヤコビ多様体とみなした場合である．2 つの写像

$$\phi_j:\ (\mathcal{D}=)\,\mathcal{C}\to\mathcal{C} \qquad (j=1,2),$$

ϕ_1 は $\boldsymbol{x}\to\boldsymbol{x}$，$\phi_2$ は $\boldsymbol{x}\to-\boldsymbol{x}$ を考えよう．両者ともコサイクル $\boldsymbol{a}_\sigma$ は恒等的に 0 である．前者の場合は $\Delta_1(\boldsymbol{x}_1, \boldsymbol{x}_2)=\boldsymbol{x}_1-\boldsymbol{x}_2$ であり，後者の場合は $\Delta_2(\boldsymbol{x}_1, \boldsymbol{x}_2)=\boldsymbol{x}_2-\boldsymbol{x}_1$ である．この 2 つは $\mathcal{C}=\mathcal{D}$ の自己同型 $\boldsymbol{x}\to-\boldsymbol{x}$ で互いにうつりあう．

この例は $H^1(\Gamma, \overline{\mathfrak{G}})$ の自明な元に対応している．同様の現象は $H^1(\Gamma, \overline{\mathfrak{G}})$ の位数 2 の元に対しても起こる(かつこのときに限る)[読者の演習問題 !]．

この困難さを扱うため，双有理同値な 2 つの主等質空間の構造をもつものは同一視することにする．これにより $H^1(\Gamma, \overline{\mathfrak{G}})$ の各元が一意的な主等質空間の構造を定めることになる．

逆に，主等質空間の構造は $H^1(\Gamma, \overline{\mathfrak{G}})$ の元を定める．写像

$$\phi:\ \mathcal{D}\to\mathcal{C}$$

を考えてみよう．もともとの構成法により，対応するコサイクルは

$$\boldsymbol{a}_\sigma=(\sigma\phi)(\boldsymbol{\xi})=\phi(\boldsymbol{\xi})$$

で与えられた．ここで $\boldsymbol{\xi}$ はガロア群の作用で固定される $\mathcal{D}$ の生成点である．

さて，$\boldsymbol{\alpha}$ は $\mathcal{D}$ の代数的な点(例えば $\overline{\boldsymbol{Q}}$ 上定義された $\mathcal{D}$ の点)としよう．ガロア群の元 σ は $\boldsymbol{\alpha}$ と写像 ϕ の係数に作用するので

$$\sigma(\phi(\boldsymbol{\alpha}))=(\sigma\phi)(\sigma\boldsymbol{\alpha})=\phi(\sigma\boldsymbol{\alpha})+\boldsymbol{a}_\sigma$$

を得る．したがって，

$$\begin{aligned}\Delta(\boldsymbol{\alpha}, \sigma\boldsymbol{\alpha})&=\phi(\boldsymbol{\alpha})-\phi(\sigma\boldsymbol{\alpha})\\&=\phi(\boldsymbol{\alpha})-\sigma(\phi(\boldsymbol{\alpha}))+\boldsymbol{a}_\sigma\end{aligned}$$

を得る．こうして，$\{\Delta(\boldsymbol{\alpha}, \sigma\boldsymbol{\alpha})\}_\sigma$ はコサイクルであり，$\{\boldsymbol{a}_\sigma\}_\sigma$ とはコバウンダリーだけ違っている．

以上をまとめて次の定理を得る．

定理 $\boldsymbol{Q}$ 上の主等質空間 $(\mathcal{D}, \Delta)$（の $\boldsymbol{Q}$ 上の双有理同値類）と $H^1(\Gamma, \overline{\mathfrak{G}})$ の元との間には標準的な同型がある．$(\mathcal{D}, \Delta)$ に対応する $H^1(\Gamma, \overline{\mathfrak{G}})$ の元はコサイクル $\{\Delta(\boldsymbol{\alpha}, \sigma\boldsymbol{\alpha})\}_\sigma$ で与えられる．ここで $\boldsymbol{\alpha}$ は $\mathcal{D}$ の任意の代数的な点である． □

注意 1 主等質空間は Weil によって導入された．彼は $H^1(\Gamma, \overline{\mathfrak{G}})$ を使わずに群構造を直接定義した．

注意 2 （進んだ読者のために）ヤコビ多様体は複素数体上定義された古典的なヤコビ多様体の精密化である．

$\mathcal{D}$ 上の因子 $\mathfrak{a}$ は $\mathcal{D}$ 上の代数的点 $\boldsymbol{\alpha}$ たちから $\boldsymbol{Z}$ への写像で，有限個の $\boldsymbol{\alpha}$ 以外では 0 であるようなものであったことを思い起こそう．因子はガロア群 $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ の作用で（普通の意味で）不変であるとき，$\boldsymbol{Q}$ 上定義されているという．$\mathfrak{a}$ が写像 $\boldsymbol{\alpha} \to n_{\boldsymbol{\alpha}}$ で与えられているとき，次数 $\sum n_{\boldsymbol{\alpha}}$ で与えられる．

因子 $\mathfrak{a}$ の次数は 0 であるとしよう．ヤコビ多様体への写像とは

$$\mathrm{Jac}\,(\mathfrak{a}) = \sum_{\boldsymbol{\alpha}} n_{\boldsymbol{\alpha}} \phi(\boldsymbol{\alpha}) \in \overline{\mathfrak{G}}$$

で与えられる $\mathfrak{a}$ から $\overline{\mathfrak{G}}$ への写像である．右辺の和は楕円曲線 $\mathcal{C}$ での和を意味する．

因子 $\mathfrak{a}$ は，その重複度も込めて $\phi(\boldsymbol{\alpha})$ が $\mathcal{C}$ 上の関数の極と零点であるとき，かつそのときに限り，この写像の核に属する．ϕ によって $\mathcal{D}$ と $\mathcal{C}$ とを同一視すると，これは $\mathfrak{a}$ が $\mathcal{D}$ 上の関数から定まる因子（**主因子**）であることと同じである．

$\mathfrak{a}$ が $\boldsymbol{Q}$ 上定義されていれば $\mathrm{Jac}\,(\mathfrak{a})$ も $\boldsymbol{Q}$ 上定義されている．これは $\sigma\phi(\boldsymbol{\alpha})$ に関する公式から容易に導くことができる．したがって，群の中への同型写像

$$\frac{\{\boldsymbol{Q}\text{ 上定義された次数 }0\text{ の }\mathcal{D}\text{ 上の因子}\}}{\{\text{主因子}\}} \to \mathfrak{G}$$

が定まる．

最後に次のことを述べてこの章を終えよう．次数 0 の因子 $\mathfrak{a}$ が $\boldsymbol{Q}$ 上定義され，かつ主因子であるとすると，それは $\mathcal{D}$ 上の $\boldsymbol{Q}$ 上定義された関数の定める因子である．なぜなら，関数 f は $\overline{\boldsymbol{Q}}$ 上定義され因子 $\mathfrak{a}$ を定めるとしよう．$\sigma \in \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ に対して $\mathfrak{a}$ は σf の因子でもあるので

$$\frac{\sigma f}{f} \in \overline{\boldsymbol{Q}}^*$$

である．$\sigma \to \sigma f/f$ が $\overline{\boldsymbol{Q}}^*$ に値をとるコサイクルであることを示すのは容易であり，Hilbert の定理 90［第 20 章演習問題 5］より，コバウンダリーである．したがって，すべての σ に対して $\sigma f/f = \sigma\lambda/\lambda$ となるような $\overline{\boldsymbol{Q}}^*$ の元 λ が存在する．すると $\lambda^{-1}f$ はガロア群で固定され，$\boldsymbol{Q}$ 上定義されているとすることがわかる．［もちろん以上の注意は一般的に正しく任意の種数の曲線に対して適用できる.］

【演習問題】

1　$\boldsymbol{\xi}, \boldsymbol{x}$ をそれぞれ $\mathcal{D}, \mathcal{C}$ のガロア群で固定される生成点とするときに，関数 $A(\boldsymbol{\xi}, \boldsymbol{x}) = \phi^{-1}(\phi(\boldsymbol{\xi}) + \boldsymbol{x})$ は $\boldsymbol{Q}$ 上定義されていることを示し，その性質を調べよ．

23

Tate–Shafarevich 群

前の 2 章の結果をまとめてみよう.

以前と同様に, $\boldsymbol{Q}$ 上定義された楕円曲線

$$\mathcal{C}:\ Y^2 = X^3 + AX + B$$

を考える. $\mathcal{C}$ の $\boldsymbol{Q}$ 上定義された点, $\overline{\boldsymbol{Q}}$ 上定義された点のなす群をそれぞれ $\mathfrak{G}$, $\overline{\mathfrak{G}}$ と記し, $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ を Γ と記す. 1 次元コホモロジー群 $H^1(\Gamma, \overline{\mathfrak{G}})$ は $\{\mathcal{D}, \Delta\}$ の同値類と標準的に同型である. ここで $\mathcal{D}$ は種数 1 の曲線であり, Δ はその上の主等質空間の構造を与えている. この群はしばしば Weil–Châtelet 群とよばれ, $WC = WC(\mathcal{C})$ と記される.

正整数 $m > 1$ に対して群 $\overline{\mathfrak{G}}$ の任意の元 $\boldsymbol{a}$ は m で割り切れる. なぜなら, $m\boldsymbol{b} = \boldsymbol{a}$ をみたす $\boldsymbol{b}$ を求めるには代数的な方程式を解けばよいからである. 前章の完全列は

$$0 \to \mathfrak{G}/m\mathfrak{G} \to H^1(\Gamma, \Delta_m) \to \left[H^1(\Gamma, \overline{\mathfrak{G}})\right]_m \to 0$$

となる. ここで $\Delta_m\ (\subset \overline{\mathfrak{G}})$ は $\overline{\mathfrak{G}}$ の位数 m の元全体であり, $[\cdots]_m$ は位数が m の約数である元のなす部分群を意味する.

さて, 状況は弱い意味の Mordell–Weil の定理に近づいている. $\mathfrak{G}/m\mathfrak{G}$ の像である $H^1(\Gamma, \Delta_m)$ の部分群を見いだしたい. 上の列が完全であることから, これらの元は写像

$$H^1(\Gamma, \Delta_m) \to H^1(\Gamma, \overline{\mathfrak{G}}) = WC(\mathcal{C})$$

の核とちょうど一致することがわかる. 核の元であることは像は自明な主等

質空間 $\{\mathcal{D}, \Delta\}$ であること，すなわち，$\mathcal{D}$ 上に $\boldsymbol{Q}$ 上定義された点があることを意味する．

$m=2$ のときは弱い意味の Mordell–Weil の定理での議論にもどることになる．そこでは $H^1(\Gamma, \Delta_2)$ の像である $\{\mathcal{D}, \Delta\}$ に現れる曲線 $\mathcal{D}$ は 2 個の 2 次曲面の交わりであることを示した[*1]．

すでに強調したことであるが，現在に至るまで $\mathcal{D}$ 上に有理点があるか否かを判定するアルゴリズムは存在しない．しかしながら，局所的にいたるところ $\mathcal{D}$ 上に有理点があるかどうかを決めることは難しくない．以下で示すように，局所的にいたるところで有理点があるような $\mathcal{D}$ が定める WC の元全体は群をなす．この群は Tate–Shafarevich 群とよばれ，通常ロシア文字 Ш (シャー) で示される[*2]．

Ш が部分群であることを示すには，局所化に関して論じる必要がある．任意の素数 p (∞ も含む) に関し，$\boldsymbol{Q}$ 上でなく $\boldsymbol{Q}_p$ 上定義された対象を表すのに添え字 p を用いる．$\boldsymbol{Q}$ 上定義された主等質空間 $\{\mathcal{D}, \Delta\}$ の同値類に対して同じ同値類 $\{\mathcal{D}, \Delta\}$ を $\boldsymbol{Q}_p$ 上で考えることによって，自然な写像

$$j_p: \ WC \to WC_p$$

が定まる．主等質空間の積(合成)の非コホモロジー的記述は基礎体 $\boldsymbol{Q}$ 上で可能であり，このことより直ちに局所化 j_p は群構造を保つことがわかる．ただし，この合成則については今だ述べてはいない．コホモロジーの観点からは，埋め込み $\overline{\mathfrak{G}} \subset \overline{\mathfrak{G}}_p$ より定まる写像

$$j_p: \ H^1(\Gamma, \overline{\mathfrak{G}}) \to H^1(\Gamma_p, \overline{\mathfrak{G}}_p)$$

がある．この状況は第 21 章の末部で論じた．そこでは j_p は群の準同型であり，この写像 j_p は埋め込み $\overline{\boldsymbol{Q}} \subset \overline{\boldsymbol{Q}}_p$ にはよらないことを示した．

Ш がすべての局所化写像 j_p ($p=\infty$ を含む) の核の共通部分であるのは明ら

＊1　主等質空間を記す Δ と $\overline{\mathfrak{G}}$ の位数 2 の元のなす群 Δ_2 に紛らわしい記号を使ったことをおわびしたい．

＊2　これは著者のこの方面に関する貢献でもっとも長もちしているものである．Tate によれば最初の表現は TS だったそうである．これは WC という記号の続編であって，アメリカでは “tough shit” というのはもっとも消去しづらいものという意味なのである．

かである．与えられた m に対して，$Ш \subset H^1(\Gamma, \overline{\mathfrak{G}})$ にうつされる $H^1(\Gamma, \Delta_m)$ の元全体のなす部分群を S_m と記す．S_m は m 次 Selmer 群とよばれる．こうして完全列

$$0 \to \mathfrak{G}/m\mathfrak{G} \to S_m \to [Ш]_m \to 0$$

が得られた．

弱い意味の Mordell–Weil の定理の証明で用いた $m=2$ の場合，S_2 は有限であり，効果的に構成できることを示した．もっと複雑にはなってくるが，同様の議論を用いて一般に m に対しても同様の結果を S_m に対して示すことができる．ただ，うまく構成できるかということについては，実用的ではなくなってくる．

以上をまとめておこう．Selmer 群は本質的にはわかる．それはおおむね $\mathfrak{G}/m\mathfrak{G}$ であり，補正項（$\mathfrak{G}/m\mathfrak{G}$ と Selmer 群との差）は Ш で与えられる．それは与えられた $\mathcal{C}$ をヤコビ多様体としてもつ種数 1 の曲線に局所–大域原理（Hasse の原理）の成立に関する障害を与えている．

これがこの理論で到達できる限界である．この理論の背後を説明することでこの章を終ろう．

この理論が見いだされる前に，Selmer は楕円曲線，特に

$$\mathcal{C}: \ X^3+Y^3+dZ^3=0 \qquad (d \in \boldsymbol{Z})$$

の形の曲線の Mordell–Weil 群を見いだすための研究に手をつけていた．彼は Mordell–Weil 群の上限を求めるのに降下法を使った．また彼は $\mathcal{C}$ 上の有理点を直接見いだし，Mordell–Weil 群の階数を下からおさえた．この階数に関する上限と下限とはほとんど一致し，不一致のときはその差は常に偶数であった．また，他の降下法（例えば，$\mathfrak{G}/2\mathfrak{G}$ と $\mathfrak{G}/3\mathfrak{G}$ の評価など）から得られる階数の評価は，それらが違っているとしても常に偶数の違いであった．

Tate と Shafarevich によって群 Ш が発見され，この現象を Ш の構造を使って説明しようと試みることは自然なことである．Ш 上には歪対称形式が存在し，その核は無限に割れる元の全体のなす群になることが知られている．無限に割れる元が Ш にあることは不自然であると考えられ，現在のところ，証明はできないがそのような元は存在しないと思われるたくさんの状況証拠

がある．もし無限に割れる元がなければ，歪対称形式の存在から$[\text{Ш}]_m$の位数は平方数であることがわかる．このことからSelmerの見いだしたことが説明できる．

種数0の曲線に対する局所–大域原理は単なる原理ではなくて，質的な(quantitative)定式化が知られている(しかも，もっと一般に線型代数群に対しても同様の事実が知られている．現在では“玉河数”を使って定式化されている)．(コンピューターを用いた)膨大な計算によってBirchとSwinnerton-Dyerは楕円曲線に対する質的な(quantitative)局所–大域定理とみなされるものを提出した．彼らの公式中にはそう見なければ説明のつかない数が現れる．彼らのすべての計算では，この不思議な数は整数であり，しかも平方数であった．

この数をШの位数(有限であると仮定した上での話しだが)と解釈するのは自然である．そして一度，このような解釈ができると，このことは別の観点からも支持されることとなった．

Birch–Swinnerton-Dyer予想は広く一般化され，その正しさについてはさらにいくつかの証拠が挙げられている．ここ数年，その証明について初めて実質的な進歩があった．ごく最近，RubinとKolyvaginがある種の楕円曲線に対してШの有限性を証明するまで，そのような楕円曲線は1つも知られていなかったのである．

【演習問題】

1　$m|n$を満足する整数m, nに対して以下の図式を可換とする群の準同型λが存在することを示せ．

$$\begin{array}{ccc} \mathfrak{S} & \to & H^1(\Gamma, \Delta_n) \\ & \searrow & \downarrow \lambda \\ & & H^1(\Gamma, \Delta_m) \end{array}$$

これより以下の完全系列のなす図式を可換とするμ, νが存在することを示せ．

$$\begin{array}{ccccccccc} 0 & \rightarrow & \mathfrak{G}/n\mathfrak{G} & \rightarrow & H^1(\Gamma, \Delta_n) & \rightarrow & [WC]_n & \rightarrow & 0 \\ & & \downarrow \mu & & \downarrow \lambda & & \downarrow \nu & & \\ 0 & \rightarrow & \mathfrak{G}/m\mathfrak{G} & \rightarrow & H^1(\Gamma, \Delta_m) & \rightarrow & [WC]_m & \rightarrow & 0 \end{array}$$

μ, ν を実際に書き下せ.

24

自己準同型環

この章では基礎体 k は任意とする．ときとして $p \neq 2, 3$ を仮定する（この制限は単に標準形のとり方による）．主要な目標は有限体上の点の個数の評価であるが，もう少し広い背景のもとで考察する．

体 k 上で定義された楕円曲線

$$\mathcal{C}:\ Y^2 = X^3 + AX + B$$

を考えよう．k 上定義された写像

$$\phi:\ \mathcal{C} \to \mathcal{C}$$

で

$$\phi(\boldsymbol{o}) = \boldsymbol{o}$$

をみたすものを（k 上の）$\mathcal{C}$ の自己準同型という．

特別な準同型として $\mathcal{C}$ のすべてを $\boldsymbol{o}$ にうつす定数自己準同型がある．それ以外では，$\mathcal{C}$ の生成点 $\boldsymbol{x}$ に対して

$$\boldsymbol{\xi} = \phi(\boldsymbol{x})$$

も生成点であり，$k(\boldsymbol{x})/k(\boldsymbol{\xi})$ は代数拡大である．ϕ の次数を

$$d(\phi) = [k(\boldsymbol{x}) : k(\boldsymbol{\xi})]$$

で定義する．定数自己準同型の次数は 0 と約束する．

最初の補題は，ϕ は $\mathcal{C}$ の群構造を保存するというものである．これは後で本質的には必要とはならないが，その考え方は有用である．有限体への応用ではその結論は明らかであろう．

補題 1 $\mathcal{C}$ 上の点 $\boldsymbol{a}, \boldsymbol{b}$ に対して

$$\phi(\boldsymbol{a}+\boldsymbol{b}) = \phi(\boldsymbol{a})+\phi(\boldsymbol{b})$$

が成り立つ.

［証明の概略］ 必要に応じて基礎体を拡大して $\boldsymbol{a}, \boldsymbol{b}$ は k 上定義されていると仮定してよい. ϕ が定数自己準同型のときは補題は明らかであり, 証明を要しない. それ以外のとき, 生成点 $\boldsymbol{x}$ に対して $\boldsymbol{\xi}=\phi(\boldsymbol{x})$ とおく. 群構造の定義より $\boldsymbol{a}, \boldsymbol{b}$ でのみ 1 位の零点をもち, $\boldsymbol{o}, \boldsymbol{a}+\boldsymbol{b}$ でのみ 1 位の極をもつ

$$\lambda = \lambda(\boldsymbol{x}) \in k(\boldsymbol{x})$$

が存在する.

$$\Lambda = \Lambda(\boldsymbol{\xi}) = \mathrm{Norm}_{k(\boldsymbol{\xi})/k(\boldsymbol{x})}\lambda$$

とおくと, Λ は $\phi(\boldsymbol{a}), \phi(\boldsymbol{b})$ でのみ 1 位の零点をもち, $\phi(\boldsymbol{a}+\boldsymbol{b}), \boldsymbol{o}=\phi(\boldsymbol{o})$ でのみ 1 位の極をもつ. ▮

注意 第 14 章の補題 1 を参照のこと. 上の証明では Silverman, 定理 4.8 (p. 75)によった. そこでは同種写像に対して証明されており, 完全である. 任意次元のアーベル多様体に対しては, D. Mumford: *Abelian varieties*, Oxford, 1970, p.43, 系 3, または H. P. F. Swinnerton-Dyer: *Analytic theory of abelian varieties*, Cambridge, 1974, 定理 32, または S. Lang: *Abelian varieties*, New York & London, 1959, 第 II 章定理 4 を参照されたい.

以下で必要なのは次の系である.

系 $\boldsymbol{x}, \boldsymbol{\xi}$ は上の通りとし,

$$\boldsymbol{x} = (x, y), \quad \boldsymbol{\xi} = (\xi, \eta)$$

であるとする. このとき $\xi \in k(x)$ でありかつ

$$[k(x) : k(\xi)] = [k(\boldsymbol{x}) : k(\boldsymbol{\xi})] = d(\phi)$$

である.

［証明］ $\phi(-\boldsymbol{x}) = -\phi(\boldsymbol{x}) = -\boldsymbol{\xi}$ であるから. ▮

任意の 2 個の自己準同型 ϕ, ψ に対して, 和 $\phi+\psi$ および積 $\phi\psi$ を

$$(\phi+\psi)(\boldsymbol{x}) = \phi(\boldsymbol{x})+\psi(\boldsymbol{x}),$$
$$(\phi\psi)(\boldsymbol{x}) = \phi(\psi(\boldsymbol{x}))$$

で定義する. ここで $\boldsymbol{x}$ は生成点である. この定義により自己準同型全体のな

す集合は(必ずしも可換とは限らない)環の構造を定めることが容易にわかる.

補題 2

$$d(\phi\psi) = d(\phi)d(\psi).$$

［証明］　明らか. ∎

補題 3

$$d(\phi+\psi)+d(\phi-\psi) = 2d(\phi)+2d(\psi).$$

［証明］　生成点 $\boldsymbol{x}=(x,\,y)$ に対して

$$\begin{aligned}\phi(\boldsymbol{x}) &= \boldsymbol{\xi}_1,\\ \psi(\boldsymbol{x}) &= \boldsymbol{\xi}_2,\\ (\phi+\psi)(\boldsymbol{x}) &= \boldsymbol{\xi}_3,\\ (\phi-\psi)(\boldsymbol{x}) &= \boldsymbol{\xi}_4\end{aligned}$$

とおくと

$$\boldsymbol{\xi}_3 = \boldsymbol{\xi}_1+\boldsymbol{\xi}_2, \quad \boldsymbol{\xi}_4 = \boldsymbol{\xi}_1-\boldsymbol{\xi}_2$$

である. ここで $\boldsymbol{\xi}_j=(\xi_j,\,\eta_j)$ $(j=1,2,3,4)$ とおくと

$$\xi_j \in k(x) \qquad (j=1,2,3,4)$$

である.

高さに関する対応する結果(第 17 章補題 4)と同様に論じることができる. $k(x)$ の元の次数は $\boldsymbol{Q}$ の元の高さに対応する. $k(x)$ には k 上自明であるアルキメデス的付値は存在しないので, 対応する結果はさらに精密になる.

和と差の公式により

$$\begin{aligned}&1:\xi_3+\xi_4:\xi_3\xi_4 =\\ &(\xi_1-\xi_2)^2:2(\xi_1\xi_2+A)(\xi_1+\xi_2)+4B\\ &\qquad\qquad :\xi_1^2\xi_2^2-2A\xi_1\xi_2-4B(\xi_1+\xi_2)+A^2\end{aligned}$$

が成り立つ. 高さの場合と同様の議論により[*1]

$$\deg(\xi_3)+\deg(\xi_4) = 2\deg(\xi_1)+2\deg(\xi_2)$$

を得る. ここで "deg" は x の有理関数としての次数(＝分子と分母の次数のうち大きい方)を意味する.

---

*1　第 17 章の(*)も参照のこと.

したがって，補題1の系により補題が示された. ∎

系　すべての $m, n \in \boldsymbol{Z}$ に対して

$$d(m\phi+n\psi) = rm^2+smn+tn^2$$

が成立するような ϕ, ψ に依存する $r, s, t \in \boldsymbol{Z}$ が存在する．さらに

$$r \geqq 0, \quad t \geqq 0, \quad s^2-4rt \leqq 0$$

である.

［証明］　最初の部分は高さの場合と同様にして示される*2．2番目の部分は定義より $d \geqq 0$ であるので，m, n に関する2次形式は正定値もしくは半正定値であることより従う. ∎

この章の以下の部分は有限体上の場合への応用には必要ない.

いささか記号の濫用になるが，定数自己準同型を0で，恒等自己準同型 $\phi(\boldsymbol{x})=\boldsymbol{x}$ を1で表すことにする.

補題4　任意の自己準同型 ϕ は2次方程式

$$\phi^2-s\phi+t=0 \qquad (s, t \in \boldsymbol{Z})$$

を満足する.

［証明］　前の補題により，すべての $m, n \in \boldsymbol{Z}$ に対して

$$d(m+n\phi) = m^2+smn+tn^2$$

が成り立つような $s, t \in \boldsymbol{Z}$ が存在する.

整数 $l \in \boldsymbol{Z}$ に対して

$$d(\phi+l) = d(\phi-s-l) = l^2+sl+t$$

が成り立つ．したがって，補題2より

$$d((\phi+l)(\phi-s-l)) = (l^2+sl+t)^2 \qquad (*)$$

が成り立つ．一方,

$$(\phi+l)(\phi-s-l) = \phi^2-s\phi-l(s+l) \qquad (**)$$

である．したがって，補題3の系で ϕ, ψ をそれぞれ $\phi^2-s\phi$, 1 ととることによって，すべての $n \in \boldsymbol{Z}$ に対して

$$d(\phi^2-s\phi+n) = (-n+t)^2$$

*2　第17章演習問題2も参照のこと.

である．特に

$$d(\phi^2-s\phi+t)=0$$

が成り立つ．しかし次数 0 の自己準同型は定数自己準同型 0 のみである． ∎

注意 Deuring によって示されたように，自己準同型環は次のいずれかと同型である．

（i） $\boldsymbol{Z}$

（ii） 虚 2 次体の整数環

（iii） 一般化された 4 元数体の整数環

この 3 番目の場合は標数 $p\neq 0$ のときのみおこり，非可換体は非常に特別なものである．

【演習問題】

1 基礎体は $i^2=-1$ となる元 i を含んでおり，かつ標数は 2 でないと仮定する．$A\neq 0$ のとき楕円曲線 $\mathcal{C}$: $Y^2=X^3+AX$ を考える．このとき，写像

$$\varepsilon:\ Y\to iY,\quad X\to X$$

は自己準同型であることを示せ．

自己準同型 $1+\varepsilon$ を構成し，自己準同型として $(1+\varepsilon)^2=2\varepsilon$ であることを示せ．

2 基礎体は標数 2, 3 以外であり，かつ $\rho\neq 1$, $\rho^3=1$ をみたす元 ρ を含んでいるとする．$B\neq 0$ のとき楕円曲線 $\mathcal{C}$: $Y^2=X^3+B$ を考える．このとき，

$$\lambda:\ X\to\rho X,\quad Y\to Y$$

は自己準同型であることを示せ．自己準同型 $\lambda-\lambda^2$ を構成し，自己準同型として $(\lambda-\lambda^2)^2=-3$ であることを示せ．

3 基礎体の標数は 2 ではないとする．$a\neq 0$ に対して 2 つの曲線

$$\mathcal{C}:\ Y^2=X(X^2+aX+b)$$
$$\mathcal{C}_1:\ Y^2=X(X^2-2aX+a^2-4b)$$

が代数閉体上同種であるように b を定める．このとき，-2 が基礎体で平方数でなければ $\mathcal{C}$ と $\mathcal{C}_1$ とは基礎体上同種であることを示せ．

この同種を $\mathcal{C}$ 上の自己準同型と考え，μ と記す．自己準同型として $\mu^2=-2$ であることを示せ．

4 自己準同型 ϕ: $\mathcal{C}\to\mathcal{C}$ に対して

$$\phi^2 - s\phi + t = 0, \qquad s, t \in \boldsymbol{Z}$$

が成り立つとする．正整数 m に対して $\psi = \phi^m$ は

$$\psi^2 - s_m \psi + t_m = 0$$

をみたすことを示せ．ここで $s_m, t_m \in \boldsymbol{Z}$ は次のように定義される．$T^2 - sT + t = 0$ の解を $\alpha, \beta \in \overline{\boldsymbol{Q}}$ とすると，

$$s_m = \alpha^m + \beta^m, \quad t_m = \alpha^m \beta^m.$$

5

（i） 自己準同型 ϕ に対して，ϕ' を $\phi \in \boldsymbol{Z}$ のとき

$$\phi' = \phi,$$

それ以外のときは $\phi^2 - s\phi + t = 0$ をみたすような s を用いて，$\phi' = s - \phi$ と定義する．

$$\phi\phi' = \phi'\phi = d(\phi)$$

を示せ．

（ii） $\mathcal{C}$ の生成点 $\boldsymbol{x}$ と，$\phi(\xi_j) = \boldsymbol{x}$ を満足する $\overline{k(\boldsymbol{x})}$ (k は基礎体) 上の点 $\xi_1, \cdots, \xi_t$（ただし，ϕ が非分離的なときは適当に定数倍する）に対して

$$\phi'(\boldsymbol{x}) = \sum_j \boldsymbol{\xi}_j$$

を示せ（ただし，$\sum$ は $\mathcal{C}$ の加法である）．

（iii） 他の自己準同型 ψ に対して

$$(\phi\psi)' = \psi'\phi'$$
$$(\phi + \psi)' = \phi' + \psi'$$

を示せ．

6 k 上超越的な t に対して体 $K = k(t)$ および k 上定義された楕円曲線 $\mathcal{C}$ を考える．$\mathcal{C}$ 上の点 (ξ, η) が K 上定義されていれば k 上定義されていることを示せ．

[ヒント．$\mathcal{C}$ が $Y^2 = F(X)$ で定義されているとき s を $s^2 = F(t)$ として決める．補題 1 を $\mathcal{C}$ から $\mathcal{C}$ への写像 $(t, s) \to (\xi, \eta)$ に適用せよ．

注意．M. Reid: *Undergraduate algebraic geometry*, LMS Student Texts **12**) p.28 を参照のこと．

問題． Reid の証明の動機づけを与えよ．]

25

有限体上定義された楕円曲線の有理点

$\boldsymbol{F}_q$ は q 個の元からなる体とし，その標数を p で表す．したがって，q は p のベキ乗である．最初の目標は次の定理である．

定理 1

$$\mathcal{C}:\ Y^2 = X^3 + AX + B$$

は有限体 $\boldsymbol{F}_q$ 上定義された楕円曲線とする．$\mathcal{C}$ の $\boldsymbol{F}_q$ 上定義された点の個数を N とすれば，N は

$$|N-(q+1)| \leqq 2q^{1/2}$$

をみたす． □

ここでは証明の主なアイデアを述べるが，その内容の 1 つは非常に興味深いものである．また，この章では用いている標準系の関係上，$p \neq 2, 3$ である．N 個の点は無限遠点 $\boldsymbol{o}$ を含んでいることに注意しよう．この章の終りで，他のいくつかの結果の証明を述べる．

$\boldsymbol{x} = (x, y)$ は生成点とする．まず，$\phi(\boldsymbol{x}) = (x^q, y^q)$ は，また，曲線上にあることを示す．実際，$p|q$ であり，$A^q = A$, $B^q = B$ であるから，

$$\begin{aligned}(y^q)^2 &= (x^3 + Ax + B)^q \\ &= (x^q)^3 + A^q x^q + B^q \\ &= (x^q)^3 + Ax^q + B\end{aligned}$$

である．これは **Frobenius 準同型**とよばれるものである．

さて，$\boldsymbol{u}=(u,v)$ は代数閉包 $\overline{\boldsymbol{F}}_p$ 上定義された点である．すると

$$\phi(\boldsymbol{u})=(u^q,\ v^q)$$

であるから，$\boldsymbol{u}$ は ϕ で固定されるとき，または同じことだが，

$$(\phi-1)\boldsymbol{u}=\boldsymbol{o}$$

となるときに限り，$\boldsymbol{F}_q$ 上定義される．ここで，1 は恒等自己準同型であり，$\phi-1$ は自己準同型環の中で定義されたものである．

前章の記号を用いれば，明らかに，

$$d(\phi)=q$$

であり，第 24 章補題 3，系から

$$d(\phi-1)=q-s+1,$$

ただし，

$$s^2 \leqq 4q, \quad |s| \leqq 2q^{1/2}$$

である．

すでに述べたように，$\overline{\boldsymbol{F}}_q$ 上定義された点は，$\phi-1$ の核になっているときに限り，$\boldsymbol{F}_q$ 上定義される．ところが，自己準同型の次数は核に含まれる重複度込みで数えられた代数的な点の数に等しい．ゆえに，$\phi-1$ の核の点の重複度がすべて 1 なら定理が得られる．

さて，多少の穴埋めはして欲しいのであるが，きちんと議論すれば証明するべきは以下に述べるようになることがわかる： $dx^q/dx=qx^{q-1}=0$ であり，これから $\phi-1$ の微分は -1 という自己準同型と同じになり，これは決して 0 にならない．

これから定理を得る．

注意　この結果は Hasse によるものでその証明も本質的に同様である．この結果はしばしば(種数 1 の)関数体に関する Riemann 予想とよばれる．というのは未だに未解決である(Riemann の)ゼータ関数の零点に関する Riemann 予想の類似だからである．この関数体に関する Riemann 予想は一般の種数の曲線に関しては Weil により，代数多様体に関しては Deligne により一般化された．Frobenius 写像 ϕ の作用の研究は今現在も数論幾何学の中心をなしている．

定理 2　$\mathcal{D}$ は $\boldsymbol{F}_q$ 上定義された種数 1 の曲線とする．このとき，$\boldsymbol{F}_q$ 上定義

された $\mathcal{D}$ 上の点が存在する．

［証明］ 我々は標数 0 のときにヤコビアンの理論を考えたが，同じことが一般の標数でも成立するのでこれを用いる．$\mathcal{C}$ は $\mathcal{D}$ のヤコビアンとし，$\overline{\mathfrak{G}}$ は $\overline{\boldsymbol{F}}_q$ 上定義された $\mathcal{C}$ 上の点のなす群とする．すると，

$$H^1(\Gamma, \overline{\mathfrak{G}})$$

が自明であること，ただし，

$$\Gamma = \mathrm{Gal}(\overline{\boldsymbol{F}}_q/\boldsymbol{F}_q),$$

を証明すれば十分である．

Γ は Frobenius 準同型 γ: $a \to a^q$ で生成されている*1．任意のコサイクル $\{\boldsymbol{a}_\sigma\}$ が自明であることを示そう．そのためには

$$\boldsymbol{a}_\gamma = \gamma \boldsymbol{b} - \boldsymbol{b}$$

をみたす $\boldsymbol{b} \in \overline{\mathfrak{G}}$ が存在することを示せばよい．さて，

$$\gamma \boldsymbol{b} - \boldsymbol{b} = (\phi - 1)\boldsymbol{b}$$

（ただし ϕ は幾何学的 Frobenius 写像である），したがって，$\phi-1$ は定数自己準同型ではない．今，代数閉体で考えているので，これから任意の $\boldsymbol{c} \in \overline{\mathfrak{G}}$ に対して，$(\phi-1)\boldsymbol{b} = \boldsymbol{c}$ をみたす $\boldsymbol{b}$ が存在する．特に，$\boldsymbol{c} = \boldsymbol{a}_\gamma$ としてこれが成り立つ．コサイクルの定義式から帰納的に

$$\boldsymbol{a}_\sigma = \sigma \boldsymbol{b} - \boldsymbol{b}, \quad \sigma = \gamma, \gamma^2, \gamma^3, \cdots$$

となり，定理が従う． ∎

注意　この定理の一般化については，S. Lang: Algebraic groups over finite fields. *Amer. J. Math.* **78** (1956), 535–563 を参照のこと．

上の定理は F. K. Schmidt による．その証明の背後のあるアイデアには面白いものがある．彼は $\boldsymbol{F}_{q^n}$ の拡大体上定義される点の数の評価に解析的な方法を用いた．特に，十分大きな n に対してはその数が正であることを証明した．

$\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ は $\boldsymbol{F}_{q^n}$ 上定義された n 個の共役な点とし，$\boldsymbol{c}_1, \cdots, \boldsymbol{c}_{n+1}$ は $\boldsymbol{F}_{q^{n+1}}$ 上定義された同様の点とする．すると Riemann–Roch の定理から，各 $\boldsymbol{c}_i$ で 1

*1　トポロジー的には γ がすべての有限次正規拡大のガロア群を生成しているということである．

位の極をもち，各 $\boldsymbol{b}_j$ で 1 位の零点をもつ関数が存在する．この関数はもう 1 つ零点をもち，それは $\boldsymbol{F}_q$ 上定義されてなければならないことがわかる．

定理 3

$$\lambda:\ \mathcal{C}_1 \to \mathcal{C}_2$$

は楕円曲線の間の同種写像とし，すべて $\boldsymbol{F}_q$ 上定義されているとする．N_j を $\boldsymbol{F}_q$ 上定義された $\mathcal{C}_j$ の点の数とすると，$N_1 = N_2$ が成り立つ． □

注意 同種写像は $\lambda(\boldsymbol{o}_1) = \boldsymbol{o}_2$ をみたすように定義されるものとする．

前章の補題 1 は同種写像の場合にも成り立ち，それはこの本の前の取り扱いと適合する．

［証明］ ϕ_j は $\mathcal{C}_j$ 上の Frobenius 写像とする．明らかに図式

$$\begin{array}{ccc} \mathcal{C}_1 & \xrightarrow{\phi_1} & \mathcal{C}_1 \\ \downarrow \lambda & & \downarrow \lambda \\ \mathcal{C}_2 & \xrightarrow{\phi_2} & \mathcal{C}_2 \end{array}$$

は可換である．したがって，

$$\begin{array}{ccc} \mathcal{C}_1 & \xrightarrow{\phi_1 - 1} & \mathcal{C}_1 \\ \downarrow \lambda & & \downarrow \lambda \\ \mathcal{C}_2 & \xrightarrow{\phi_2 - 1} & \mathcal{C}_2 \end{array}$$

である．これから写像の次数に関して

$$d(\phi_1 - 1) = d(\phi_2 - 1)$$

が成り立つ．ここで（定理 1 の証明より），$N_1 = N_2$ である． ∎

例 方程式

$$y^2 \equiv x(x^2 + ax + b) \pmod{p}$$

の解の数と

$$y^2 \equiv x(x^2 - 2ax + a^2 - 4b) \pmod{p}$$

の解の数は等しい．ただし a, b は整数であり，p は

$$2b(a^2 - 4b) \not\equiv 0 \pmod{p}$$

をみたす素数である． □

【演習問題】

1　p は $p\equiv 2\ (3)$ をみたす素数とする．楕円曲線

$$Y^2 = X^3+B$$

の $\boldsymbol{F}_p$ 上定義される点の数は $p+1$ であることを示せ．

［ヒント．Y を決めておいて X について解け.］

2　p は $p\equiv 3\ (4)$ をみたす素数とする．楕円曲線

$$Y^2 = X(X^2+A)$$

の $\boldsymbol{F}_p$ 上定義される点の数は $p+1$ であることを示せ．

［ヒント．$\pm X$ を一緒に考えよ.］

3　$\mathcal{C}$ は $\boldsymbol{F}_p$ 上定義された楕円曲線で，$N(n)$ は $\boldsymbol{F}_q$ 上定義される点の個数とする．ただし，$q=p^n$ である．$\overline{\boldsymbol{Q}}$ の元 α, β で

$$\alpha\beta = p$$

かつ

$$N(n) = p^n+1-\alpha^n-\beta^n$$

をみたすものがあることを示し，したがって，$N(n)$ は $N(1)$ で決まることを示せ．

$p=3$ で $\mathcal{C}$ が

$$Y^2 = X^3+X+1$$

のとき $N(2)$ を決定せよ．

［ヒント．第 24 章演習問題 4 を参照.］

4　［次の問題のための準備の問題］$\mathcal{A}$ は $\boldsymbol{Z}$ を含む，零因子をもたない可換環とする（つまり，整域）．すべての $\lambda\in\mathcal{A}$ が方程式 $\lambda^2+a\lambda+b=0$（$a, b\in\boldsymbol{Z}$ は λ に依存する）をみたすとする．このとき，$\mathcal{A}=\boldsymbol{Z}$ か，$\mathcal{A}=\boldsymbol{Z}[\alpha]$ となるような元 $\alpha\in\mathcal{A}$ が存在することを示せ．

5　$p\equiv 1\ (4)$ は素数とし，

$$\mathcal{C}:\ Y^2 = X(X^2+A)$$

は $\boldsymbol{F}_p$ 上定義された楕円曲線とする．θ は $\theta^2=-1$ をみたす $\boldsymbol{F}_p$ の元とする．このとき

$$\varepsilon:\ Y\to\theta Y,\quad X\to -X$$

は $\mathcal{C}$ の準同型で $\varepsilon^2+1=0$ をみたすことを示せ．

ϕ は Frobenius 写像とする．$\phi\varepsilon=\varepsilon\phi$ であり，$u^2+v^2=p$ をみたす適当な整数

u, v を用いて，

$$\phi = u + v\varepsilon$$

と表せることを示せ.

さらに $\boldsymbol{F}_p$ 上定義される $\mathcal{C}$ の点の数を N とすれば

$$N = p + 1 - 2u$$

となることを示せ.

適当な A と p に対して N を求め，$u = \dfrac{1}{2}(p+1-N) \in \boldsymbol{Z}$ とおけば，$u^2+v^2=p$ をみたす整数 v が存在することを示せ.

6 $p \equiv 1$ (3) は素数とし，

$$\mathcal{C}:\ Y^2 = X^3 + B$$

は $\boldsymbol{F}_p$ 上定義された楕円曲線とする．θ は $\theta^3=1$，$\theta \neq 1$ をみたす $\boldsymbol{F}_p$ の元とする．このとき

$$\lambda:\ Y \to Y, \quad X \to \theta X$$

は $\mathcal{C}$ の準同型で $\lambda^2+\lambda+1=0$ をみたすことを示せ.

ϕ は Frobenius 写像とする．$\phi\lambda = \lambda\phi$ を示せ．以下，前問と同様のことを考えよ.

7 $\boldsymbol{F}_p$ 上定義された楕円曲線

$$\mathcal{C}:\ Y^2 = X(X^2 + 4CX + 2C^2)$$

を考える．ここで p は -2 が平方剰余であるような素数とする．$\boldsymbol{F}_p$ 上定義される点の数 N は適当な整数 u を用いて

$$N = p + 1 - 2u$$

の形に書けることを示せ．また，この u に関し，

$$u^2 + 2v^2 = p$$

をみたす整数 v が存在することを示せ.

［ヒント．第 24 章演習問題 3 を参照.］

26

楕円曲線を用いた因数分解

与えられた大きな整数の素因数を見つける問題は，古来数学者の興味を引き続けてきた．近年，この問題は実用的，さらに“政治的”な様相を呈してきた．というのは，暗号論で大きな素数の積を利用することが重要になってきたからである．

普通，(いつも必ずというわけではないが)与えられた合成数 n が合成数であることを証明するのはやさしい．例えば，適当な整数 $a>1$ に関して $a^{n-1}\not\equiv 1 \bmod n$ となれば n は素数でない．ところが，実際に非自明な素因子を見つけることはまったく別の問題なのである！

もちろん，理論的には整数 n を因数分解することは実行可能に見える．$m<n^{1/2}$ をみたす整数で割れるかどうかをテストすればよい．ところが，例えば，n が 100 桁であったりすると，これに手間取る時間は宇宙の寿命より長くなるのである．この問題で必要とされるのは実用的な方法なのである．

H. W. Lenstra は，最近楕円曲線がこの問題に対して強力な方法を与えることを示した．彼の方法の一部を簡単に紹介しよう．

Lenstra の方法は Pollard の “$p-1$ メソッド” にヒントを得ている．a は整数とし，適当な整数 k に対して，

$$m=\gcd(a^k-1,n)$$

とおく．もし $p-1|k$ ならば，$p|m$ である．よほど不運でない限り，n の他の素数がすべて m を割るということはないので，m は n の自明でない素因子

となる.

ここではもちろん a^k を実際に計算するのではなく，n を法としたものを考えるのである．$O(\log k)$ のステップの後，機能するアルゴリズムは知られている(演習問題参照)．最大公約数を求めるのはユークリッドのアルゴリズムを使えばよい.

p は素数で，$p-1$ の素因子が比較的小さなものとする．n がこのような p で割れるとき，Pollard の方法は特に有効である．その方法とはまず，次の形をした整数 k をとる*1.

$$k = k(b) = \prod_{q \leqq b} q^{e(q)},$$

ここで，q は素数であり，$q^{e(q)}$ は b 以下になる q ベキの最大のものをとる．ここで b は後で説明するような方法でとった数である.

Pollard の方法がうまくいく可能性が高いのは，n の一番小さい素因子 p がおおむね $n^{1/2}$ より小さいときである．しかしそのときでも，$p-1$ が大きい素因子をもつときはうまくいかないかもしれないのである．a の p を法とするベキ指数が実質的に $p-1$ より小さい値を見つけようとするのも可能であるが，それはあまり有望ではない.

Lenstra は，Pollard の方法が p を法とする剰余類が群構造をもつという事実によっていることを見て，楕円曲線が同様の目的に使える群構造をもつことに，気づいた.

$$\mathcal{C}: \ Y^2Z = X^3 + AXZ^2 + BZ^3$$

は楕円曲線とし，(x, y, z), $x, y, z \in \boldsymbol{Z}$ はその上の点とする.

$$k(x, y, z) = (x_k, y_k, z_k),$$

ただし，k は 1 より大きい整数とし，$x_k, y_k, z_k \in \boldsymbol{Z}$ とする．p は素数とし，$\mathcal{C}$ の $\bmod p$ 還元を考える．$\boldsymbol{F}_p$ 上の点は群をなし，その位数を

$$N = N_p = N_p(A, B)$$

とおけば

*1 つまり，k は b 以下の整数の最小公倍数である.

$$|N-(p+1)|<2\sqrt{p}$$

をみたす．$N|k$ ならば点 (x_k, y_k, z_k) を p を法としてみたものは "無限遠点" である．つまり，

$$p \mid z_k$$

である．

A, B, x, y, z が与えられると，(x_k, y_k, z_k) の値は，加法，減法，乗法を用いた $O(\log k)$ 回のステップで計算できる．ここでは同次座標を用いているので除法は必要ないのである．結果として得られた x_k, y_k, z_k は共通因子を含むかもしれないが，$N_p|k$ ならば $p|z_k$ という結論には影響しないのである．

さて，n は因数分解しようとする大きな整数とし，前のように適当な b をとってきて $k=k(b)$ とおく．すると，$\bmod n$ の加法，減法，乗法を用いた $O(\log k)$ 回のステップで x_k, y_k, z_k の $\bmod n$ での値が決まる．問題となっている n の未知の素因子 p は $N_p|k$ ならば z_k の $\bmod n$ の値を割り，また，p は

$$m=\gcd(n, z_k)$$

を割る．$z_k=0 \pmod{n}$ ならばまったく不運であるが，そうでなければ m は n の非自明な因子であり，これが求めるものであった．

もちろん，$p|n$ なるすべての $N_p \nmid k$ ならば $m=1$ である．もしそうなら，他の A, B, x, y, z（そして，場合によっては k も）をとって同様のことを繰り返すのである[*2]．

上の解説はいくつかの疑問を未解答のまま残している．

（i）　最初の曲線 C と点 (x, y, z) はどのようにして選ぶのか？　計算はすべて $\bmod n$ でなされているので，$A, B, x, y, z \in \boldsymbol{Z}$ は

$$y^2z \equiv x^3+Axz^2+Bz^3 \mod n$$

をみたすようにとれば十分である．1つの自明な方法は，$z=1$ とおき，A, x, y をランダムにとって B を決定する方法である．最初の出発点で n は小さい約数はもたないと仮定するのは自然であるから，$p|n$ なる任意の素数

＊2　曲線上で N_p がどのような値をとるかは B. J. Birch: How the number of points of an elliptic curve over a fixed prime varies. *J. London Math. Soc.* **43** (1968), 57–60 参照．

に関して $\mathcal{C}$ の $\bmod p$ 還元が楕円曲線にならないという可能性はほぼ無視できる．いずれにせよ，アルゴリズムに従って計算することはそれほど心配はない：せいぜい外れを引くといった程度である．あるいは

$$l = \gcd(n,\, 4A^3+27B^2)$$

を計算してもよい．$l=1$ なら問題はない．$1<l<n$ ならば，これは n の非自明な素因子であり，求めようとしているものである．滅多にないことであるが，$l=n$ ならば，計算を止めて新たな A, B, x, y, z を選ぶ．

（ii） $k=k(b)$ の b はどのように選ぶのが最適か？ 実はこれは n の一番小さな素因子 p によっている．もちろん，これは未知のものであるので，発見可能な方法を考えねばならない．

t は整数で $1<s<t$ とする．t のすべての素因子 q が s 以下のときに t は s–スムースであるとよばれる．T が与えられたとき，$t<T$ となる整数 t で $T^{1/u}$–スムースであるものの数は，非常におおざっぱにいって $u^{-1/u}T$ であることが知られている．

$$L = L(T) = \exp\left(\sqrt{(\log T \log\log T)}\right)$$

とおき，$0<\alpha<\infty$ とおく．$T^{1/u}=L^\alpha$ とおけば，$t \leqq T$ をみたす整数 t で L^α–スムースであるものの数は，だいたい $L^{-1/2\alpha}T$ であることがわかる．このことを次のように言いかえる：T の近傍の無作為に選んだ整数 t が L^α–スムースである確率 P は $P=L^{-1/2\alpha}$ である．

α の最良の値は後で選ぶことにする．p は n の最小の素因子とする（もちろん，これは未知の数である）．$L=L(p)$ とおく．$\mathcal{C}$ の $\bmod p$ 還元の $\boldsymbol{F}_p$ 上の点の数 $N_p=N_p(A, B)$ はだいたい p であることはすでにみた．A, B が変化するとき，N_p もしかるべくランダムにふるまうと仮定すれば，N_p が L^α–スムースであるという確率 P は $P=L^{-1/2\alpha}$ である．

$$b = L^\alpha, \quad k = k(b)$$

ととる．すると，N_p のすべての素因子は k を割る．因数分解の研究の専門家は，$N_p|k$ である可能性は非常に高いと仮定しているが，これは我々の仮定であった．アルゴリズムを 1 回実行する際のステップの数は $O(\log k)$ であるが，これは非常におおざっぱにいって $b=L^\alpha$ である．

ここでまとめをしておこう．アルゴリズムを1回実行するのにかかるステップは約 L^{α} である．1回実行しただけでうまくいく確率は約 $L^{-1/2\alpha}$ である．したがって，非自明な因子を見つけるのにかかるステップは約

$$L^{\alpha+1/2\alpha}$$

であるが，これが最小になるのは

$$\alpha = 1/\sqrt{2}$$

のときで，これが α の最良のとり方である．

今やった評価は n の未知な最小の素因子 p によっている．最悪のケースがおこるのは p が $n^{1/2}$ に近いときである．しかしながら，Lenstra のアルゴリズムがもっとも有効なのは，最小の素因子がずっと小さいときである．そのようなわけで，適当な暗号系（つまり非常に近い2つの素数の積）よりも自然にある整数 n に対する方が Lenstra の方法は有効なわけである．n の素因子に関して前もって何もわかってないときは，比較的小さな b から初めて必要なら徐々に大きくしてゆくのがよい方法である．

ここで紹介した Lenstra のアルゴリズムは，計算時間を最小にするものというものでなく，記述が簡単なものである．実際には，もっとテクニックが必要となる．ここではそれに立ち入らないが，この本の精神に従って，別の少し変化したものを1つ述べよう．

定数 $C \neq 0$ をとり楕円曲線

$$\mathcal{C}:\ CY^2 = X^3 + AX + B$$

を考える．ただし，ここでは非同次座標を用いているものとする．まず次の事実を思い出そう：(x_1, y_1) と (x_2, y_2) を曲線上の点とし，

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2),$$
$$(x_4, y_4) = (x_1, y_1) - (x_2, y_2)$$

とおけば，x_3, x_4 は係数が x_1, x_2, A, B（C は含まない）の多項式の2次方程式の根である．さて，k が正の整数，さらに記号を変えて，(x, y) は曲線 $\mathcal{C}$ 上の点で $(x_k, y_k) = k(x, y)$ とおけば，k ベキを計算する古典的なアルゴリズムは x_k を $O(\log k)$ 回のステップで計算するアルゴリズムにおきかえることができる（演習問題参照）．

ここで $X=U/V$ とおいて同次座標で考えよう．$x=u/v$ とおくと，$x_k=u_k/v_k$ である．ただし，u_k, v_k は u, v から $O(\log k)$ 回の割り算以外の四則演算で得られる．

前と同様，n は因数分解しようとする整数，p は未知の素数とする．$A, B, u, v\in\boldsymbol{Z}$ とし，$\bmod n$ で考える．すると，前と同じくして $N_p|k$ ならば，$p|v_k$ であり，$\gcd(v_k, n)$ が n の非自明な素因子であることが期待される．

このバージョンでは A, B, u, v は完全に任意に選んでよい．$x=u/v$, $y=1$ とおく．するとよほど，不運でない限り，適当に $C\in\boldsymbol{Q}$ をとれば，$\mathcal{C}$ 上に点 (x, y) が存在する．ここでは，C の具体値は必要ないので実際に求める必要はないわけである．

楕円曲線による素数判定法はその他の意外な方面で利用されている．例えば，大きな素数を法としての平方根を見つけることなどである．A. K. Lenstra and H. W. Lenstra Jr.: Algorithms in number theory, *Handbook of theoretical computer science*, vol. A (ed. J. van Leeuwen), Elsevier, 1990 の第 12 章 (pp. 673–715) 参照．

【演習問題】

1 ［次の問題への動機づけ］ G はアーベル群，n は正の整数とする．$g\in G$ に関し，g^n を計算する $O(\log n)$ 回のステップのアルゴリズムを示せ．

（i） $N=n$, $Y=1\in G$, $Z=g$

（ii） IF $N=0$, GOTO END

（iii） $M=[N/2]$, $E=N-2M$

（iv） IF $E=1$ THEN $Y=YZ$

（v） $N=M$, $Z=Z^2$

（vi） GOTO (ii)

END $[Y=g^n]$.

2 $\mathcal{C}: Y^2=X^3+AX+B$ は楕円曲線とする．正の奇数 n と $\mathcal{C}$ 上の点 $\boldsymbol{a}=(a, b)$ に対し，次の u を求める $O(\log n)$ 回のステップのアルゴリズムを確かめよ．た

だし，u は $n\boldsymbol{a}=(u, v)$ で定義する．

まず，$\boldsymbol{x}=(x, y)$ とおけば適当な？に対し $2\boldsymbol{x}=(d(x), ?)$ となるような有理関数 $d(x)$ が存在することを思い出そう．

さらに，係数が x_1, x_2 の有理式で解が x_3, x_4 であるような 2 次式

$$q(T)=q(T;\ x_1,\ x_2)$$

が存在する．ここで，x_3, x_4 は $\boldsymbol{x}_3=\boldsymbol{x}_1+\boldsymbol{x}_2$，$\boldsymbol{x}_4=\boldsymbol{x}_1-\boldsymbol{x}_2$ で定義する．

(i)　$N=n,\ X=a,\ Y=a,\ Z=a$

(ii)　IF　$N=0$,　GOTO END

(iii)　$M=[N/2],\ E=N-2M$

(iv)　$Z=d(Z)$

(v)　IF $E=1$ GOTO (viii)

(vi)　[Y が $q(T;X,Z)$ の解であることを確かめよ．]　Y IS THE OTHER ROOT OF $q(T;X,Z)$

(vii)　GOTO (ix)

(viii)　[X が $q(T;Y,Z)$ の解であることを確かめよ．]　X IS THE OTHER ROOT OF $q(T;Y,Z)$

(ix)　$N=M$

(x)　GOTO (ii)

END [$X=u$，ただし，$n(a, b)=(u, v)$].

3　適当な $E\neq 0$ をとれば点 (a, b) は曲線

$$C^*:\ EY^2=X^3+AX+B$$

上にあるとする．C^* 上で $n(a, b)=(u, v)$ とおく．u は問題 2 のアルゴリズムで与えられることを示せ．[つまり，アルゴリズムは E に無関係である．]

A

公式集

Desboves の公式[*1]　次の 3 次曲線

$$a_1X_1^3+a_2X_2^3+a_3X_3^3+dX_1X_2X_3=0$$

について考える．この曲線は $27a_1a_2a_3+d^3\neq 0$ ならば非特異である．点 $\boldsymbol{x}$ での接線の残りの点 $\boldsymbol{t}$ の座標は次の公式で与えられる．

$$t_j=x_j(a_{j+1}x_{j+1}^3-a_{j+2}x_{j+2}^3)$$

ただし j は mod 3 で考える．また，点 $\boldsymbol{x}$，$\boldsymbol{y}$ を結ぶ直線の残りの交点 $\boldsymbol{z}$ の座標は

$$z_j=x_j^2y_{j+1}y_{j+2}-y_j^2x_{j+1}x_{j+2}$$

で与えられる．ただし j は mod 3 で考える．

標準形

$$Y^2=X^3+AX+B.$$

$\boldsymbol{x}=(x,\ y)$ ならば $-\boldsymbol{x}=(x,\ -y)$．

加法公式

$$\boldsymbol{x}_1=(x_1,\ y_1),\quad \boldsymbol{x}_2=(x_2,\ y_2)$$

および

$$\boldsymbol{x}=\boldsymbol{x}_1+\boldsymbol{x}_2,\quad \boldsymbol{x}=(x,\ y)$$

とおく．

---

*1　A. Desboves: Résolution en nombres entiers et sous sa forme la plus générale, de l'équation cubique, homogène á trois inconnues. *Nouv. Ann. de la Math.*, Sér. III, vol. **5** (1886), 545–579.

$\boldsymbol{x}_2=-\boldsymbol{x}_1$ ならば，$\boldsymbol{x}=\boldsymbol{o}$ である．$\boldsymbol{x}_2=\boldsymbol{x}_1$ ならば後で述べる 2 倍の公式を用いる．そうでないときは

$$x_2 \neq x_1.$$

と仮定してよい．

$\boldsymbol{x}_1, \boldsymbol{x}_2$ を結ぶ直線の方程式は

$$Y=lX+m$$

である．ただし，

$$l=\frac{y_1-y_2}{x_1-x_2}, \quad m=\frac{x_1y_2-x_2y_1}{x_1-x_2}$$

である．この直線は楕円曲線と $\boldsymbol{x}_1, \boldsymbol{x}_2$ および

$$-(\boldsymbol{x}_1+\boldsymbol{x}_2)=-\boldsymbol{x}=(x,\ -y)$$

で交わる．x_1, x_2，および x は方程式

$$X^3+AX+B-(lX+m)^2$$

の解である．ゆえに

$$x=l^2-x_1-x_2$$

であるから，

$$(x_1-x_2)^2x=x_1x_2^2+x_1^2x_2-2y_1y_2+A(x_1+x_2)+2B$$

である．さらに

$$y=-lx-m$$

であり，したがって

$$(x_1-x_2)^3y=W_2y_2-W_1y_1$$

を得る．ただし，

$$W_1=3x_1x_2^2+x_2^3+A(x_1+3x_2)+4B$$
$$W_2=3x_1^2x_2+x_1^3+A(3x_1+x_2)+4B$$

である．

2 倍の公式　ここでは

$$(x_2,\ y_2)=\boldsymbol{x}_2=2\boldsymbol{x}=2(x,\ y)$$

を考える．もし $y=0$ ならば $\boldsymbol{x}_2=\boldsymbol{o}$ である．ゆえに

$$y \neq 0$$

として考えてよい．

$\boldsymbol{x}$ での接線を

$$Y = lX + m$$

とおく．楕円曲線の方程式を X で微分すれば

$$2Y\frac{dY}{dX} = 3X^2 + A$$

を得るので

$$l = (3x^2 + A)/2y$$

を得る．ゆえに（加法公式のときと同様にして）

$$\begin{aligned} x_2 &= l^2 - 2x \\ &= \frac{(3x^2 + A)^2 - 8xy^2}{4y^2} \end{aligned}$$

つまり，

$$x_2 = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

を得る．

y_2 を求めるためには $y = lx + m$ により決まる値

$$m = \frac{-x^3 + Ax + 2B}{2y}$$

を用いる．

$$y_2 = -lx_2 - m$$

であるから

$$\begin{aligned} (2y)^3 y_2 = x^6 &+ 5Ax^4 + 20Bx^3 \\ &- 5A^2x^2 - 4ABx - A^3 - 8B^2 \end{aligned}$$

となる．

X のみに関連した公式

$$\boldsymbol{x}_1 = (x_1, y_1), \quad \boldsymbol{x}_2 = (x_2, y_2)$$

$$x_1 \neq x_2$$

とおく．また，

$$\boldsymbol{x}_3 = \boldsymbol{x}_1 + \boldsymbol{x}_2 = (x_3,\ y_3)$$
$$\boldsymbol{x}_4 = \boldsymbol{x}_1 - \boldsymbol{x}_2 = (x_4,\ y_4)$$

とおく．すると，

$$(x_1 - x_2)^2(x_3 + x_4) = 2(x_1x_2 + A)(x_1 + x_2) + 4B,$$
$$(x_1 - x_2)^2 x_3 x_4 = x_1^2 x_2^2 - 2Ax_1x_2 - 4B(x_1 + x_2) + A^2$$

を得る．

これは加法公式の x に関する表現から従う．x_3 は公式そのものから従うし，x_4 は加法公式でたんに y_1y_2 の符号を変えたものである．ゆえに x_3+x_4 に関する公式はただちに得られる．また x_3x_4 については x_3 と x_4 をかけたものから $y_1^2y_2^2$ を消去し，$(x_1-x_2)^2$ を約せば得られる．[あるいは，第 17 章演習問題 3 参照.]

整数倍[*2]　$(X_m,\ Y_m) = m(X, Y)$，$m \in \boldsymbol{Z}$ とおく．すると，

$$X_m = \frac{X\psi_m^2 - \psi_{m-1}\psi_{m+1}}{\psi_m^2},$$

$$Y_m = \frac{\psi_{2m}}{2\psi_m^4},$$

ただし，

$$\psi_0 = 0,$$
$$\psi_1 = 1,$$
$$\psi_2 = 2Y,$$
$$\psi_3 = 3X^4 + 6AX^2 + 12BX - A^2,$$
$$\psi_4 = 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3),$$
$$\psi_{2n+1} = \psi_n^3\psi_{n+2} - \psi_{n+1}^3\psi_{n-1},$$
$$Y\psi_{2n} = \psi_n\{\psi_{n-1}^2\psi_{n+2} - \psi_{n+1}^2\psi_{n-2}\}$$

---

*2　H. Weber: *Algebra III*, § 58 参照．ただし，ここでは ψ_m の最高次の係数が常に正になるように修正してある．

である．

これは，楕円曲線上の有理関数が零点と極で定数倍を除いて決まるという事実を用いる．ここでは，局所一意化変数

$$t = X/Y$$

を用いて $\boldsymbol{o}$ での状況をみてその定数を決める．

ψ_m は以下のように定義される：

（i）　$m\boldsymbol{a}=\boldsymbol{o}$ をみたす $\boldsymbol{o}$ でないすべての $\boldsymbol{a}$ で1位の零点をもつ（$\boldsymbol{a}$ は $\overline{\boldsymbol{Q}}$ 上定義される）．

（ii）　$\boldsymbol{o}$ では mt^{-m^2+1} のようにふるまう．

より正確にいえば，

（I）　m が奇数のとき，

$$\psi_m = m\prod(X-a_j)$$

をみたす $\dfrac{1}{2}(m^2-1)$ 個の m–等分点のペア $(a_j,\ \pm b_j)$ が存在する．

（II）　m が偶数のとき，m–等分点のうち3つは2–等分点であり，

$$\psi_m = mY\prod(X-a_j)$$

$b_j \neq 0$ をみたす $\dfrac{1}{2}(m^2-4)$ 個のペア $(a_j,\ \pm b_j)$ が存在する．

また，偶奇によらず，すべての m に対して $\boldsymbol{o}$ で

$$X_m \sim m^{-2}t^{-2}, \quad Y_m \sim m^{-3}t^{-3}$$

であり，

$$\psi_m^2 X_m$$

は $\boldsymbol{o}$ 以外では極をもたない．

さらに，$(m+1)\boldsymbol{a}=\boldsymbol{o}$ または $(m-1)\boldsymbol{a}=\boldsymbol{o}$ となるときに限り，$X_m - X$ は $\boldsymbol{a}$ で消える．ゆえに

$$X - X_m = \psi_{m+1}\psi_{m-1}/\psi_m^2 \qquad (*)$$

を得る（本来ならば定数倍を除いて等しいのであるが，$\boldsymbol{o}$ で両辺とも $(m^2-1)/m^2t^2$ のようにふるまうので，定数倍の部分も等しい）．極と零点を調べれば Y_m についても同様のことが従う．

残るは最後の2つの関係式である．整数 l, m に対して，$X_l = X_m$ は $(l+m)(X,\ Y)=\boldsymbol{o}$ または $(l-m)(X,\ Y)=\boldsymbol{o}$ のときのみ成り立つ．した

がって,

$$X_l - X_m = \psi_{m+l}\psi_{m-l}/\psi_l^2\psi_m^2$$

であり,定数倍の部分は $\boldsymbol{o}$ での動きをみればわかる.ところが,

$$X_l - X_m = (X - X_m) - (X - X_l)$$

であるから,(*)より,

$$\psi_l^2\psi_{m+1}\psi_{m-1} - \psi_m^2\psi_{l+1}\psi_{l-1} = \psi_{m+l}\psi_{m-l}$$

である.$l=n$, $m=n+1$ とおけば $\psi_{m-l}=1$ であるから

$$\psi_{2n+1} = \psi_n^3\psi_{n+2} - \psi_{n+1}^3\psi_{n-1}$$

が得られ,$l=n-1$, $m=n+1$ とおけば $\psi_{m-l}=\psi_2=Y$ であるから,

$$Y\psi_{2n} = \psi_n\{\psi_{n-1}^2\psi_{n+2} - \psi_{n+1}^2\psi_{n-1}\}$$

を得る.

B

参　考　書

[1] Cassels, J. W. S.: Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.* **41** (1966), 193–291.

[2] Husemöller, D.: *Elliptic curves*, Springer, 1987.

[3] Koblitz, N.: *Introduction to elliptic curves and modular forms*, Springer, 1984.

[4] Lang, S.: *Fundamentals of diophantine geometry*, Springer, 1983.
［初版 : *Diophantine geometry*, Interscience, 1962 は少し完全ではないが一貫性がある.］

[5] Serre, J.-P.: *Lectures on the Mordell–Weil theorem*, Vieweg, 1989.
［1980–1981 の学期の講義録.］

[6] Silverman, J. H.: *The arithmetic of elliptic curves*, Springer, 1986.

[7] Tate, J.: The arithmetic of elliptic curves, *Invent. Math.* **23** (1974), 179–206.

本書を翻訳中に気がついた部分に関する参考書で原著にないものをいくつか挙げておく．まず代数幾何学については，本文を理解する上で平面代数曲線の知識があった方がよい．これに関しては以下の 2 つを挙げておく．

[8] M. Reid: *Undergraduate Algebraic Geometry*, London Mathematical Society Student Texts 12, Cambridge University Press, 1991.（邦訳）若林功（訳），初等代数幾何講義，岩波書店，1991.

[9] 上野健爾，代数幾何入門，岩波書店，1995.

[8] は本文中にも挙げられている．また [9] には平面曲線に関する丁寧な解説がある．代数幾何学に関する邦書は他にもいろいろあるがそれについては上

記の本の参考文献を見て頂きたい.

楕円曲線についてさらに続いて学ぶ場合，本書のスタイルで勉強する場合は原著に紹介してある J. W. S. Cassels: Diophantine equations with special reference to elliptic curves およびその参考文献にある Cassels 教授の一連の仕事 *Arithmetic on Curves of Genus 1 (I)–(VIII)* をお勧めする．また，J. H. Silverman: *The Arithmetic of Elliptic Curves* は多くの専門家が勧める本である．楕円曲線に関する本および文献は原著で紹介されているもの以外にもたくさんある．ここでは以下の 3 冊を挙げておく．

[10] J. H. Silverman and J. Tate: *Rational Points on Elliptic Curves*, UTM, Springer, 1992.（邦訳）足立恒雄・木田雅成・小松啓一・田谷久雄(訳)，楕円曲線論入門，シュプリンガー・東京，1995.

[11] J. H. Silverman: *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer, 1994.

[12] A. W. Knapp: *Elliptic Curves*, Math. Notes 40, Princeton University Press, Princeton, NJ, 1992.

[10] は 1961 年に著者の J. Tate が行なった楕円曲線の講義の講義録をもとに書かれたものである．本書の第 26 章に述べてあることに関してはより詳しい解説がなされている．

[11] は Silverman の前掲の著書の続編ともいえるものであってタイトルの通り "advanced" な話題が並んでいる．[12] には保型形式と楕円曲線の解説がある．

訳者あとがき

“Cassels 教授の Lectures on Elliptic Curves を邦訳しては?” と Queen's 大学の由井典子教授から勧められたのは 1992 年の夏のことであった．ちょうど，由井教授の学生さんとこの本を読んでいた私は気軽に引き受けたのだが，いざ翻訳を始めてみると何から何まで初めてづくし，なかなか大変な作業であっという間に 3 年経ってしまった．

本書の著者 J. W. S. Cassels 教授は楕円曲線に関して実例計算および一般論両面で多くの業績を挙げている数学者である（詳しくは，J. W. S. Cassels: Diophantine equations with special reference to elliptic curves およびその参考文献を参照されたい）．特に実例計算に対する著者の姿勢は本書のいたるところに現れていると思う．これは私見ではあるが，数学の学んでいく上でよい例を自分のものにしておくことが一番大切だと思う．その意味で本書を翻訳中多くのものを学ばせていただいた．

本書を翻訳中，楕円曲線の専門家でない私が翻訳を引き受けたのはやはりまずかったのではと何度か挫折しそうになったが，その度，由井典子氏に叱咤激励されなんとかここまでたどりつくことができた．氏の言葉がなければこの翻訳は完成しなかったと思う．また，京都大学の上野健爾教授には岩波書店との仲介をしていただいただけでなく本文の数章の翻訳を手助けしていただいた．その意味でこの邦訳は共訳ともいえる（ただし，妙な日本語があればそれはすべて私の責任である）．

さらに，高知大学同僚の逸見豊氏は邦訳を LATEX にて行なう際，入力の方法などで協力して下さり，同じく長沼英久氏には最初の原稿に目を通していただくなどお世話になった．4 氏と辛抱強く翻訳の原稿をまっていただいた岩波書店の宮内久男氏に心から感謝したい．

1995 年 6 月

徳 永 浩 雄

欧文索引

Artin 122
Birch 91
Blichfeldt 23
Bremner 69
Deligne 152
Deuring 149
Diophantos 1
Diophantos 幾何学 1
Fermat 1
Frobenius 準同型 151
Fueter 66
Hasse 15
Hasse 原理 2
Hensel 52
Hilbert の定理 90 120
Hypatia 1
$j(\mathcal{C})$ 118
Kolyvagin 142
Lang 153
Legendre 15
Lenstra 157
Lind 107
Mazur 64
Minkowski 23
Mordell 69
Mordell の有限生成定理 69
Mordell–Weil の有限生成定理 69
Nagell 41
p–進整数環 10
p–進体 10
p–進単数 11
p–進フィルトレーション 59
p–進付値 8
Pollard 157
$\boldsymbol{Q}$ 上定義 3
Reichardt 107
Riemann–Roch の定理 37
Riemann 予想
関数体上の—— 2
Rubin 142
Schmidt 153
Selmer 107
Selmer 群 141
Swinnerton-Dyer 91
Tate–Shafarevich 群 107
van der Corput 23
Weil 1
Weil–Châtelet 群 139

和文索引

ア

1 次元コホモロジー群 126
一般の位置 35

カ

可逆 86
可約 52

ガロアコホモロジー　113
ガロアコホモロジー論　125
還元　51
還元の核　58
関数体　75
完備　10
完備化　10
基本列　8
既約　30
極　36
局所-大域原理　2
局所化　16
局所的にいたるところで　16
群構造　33
形式　15
弦と接線の方法　30
コサイクル　114, 125
コサイクル恒等式　114, 125
コバウンダリー　115, 125
コホモローグ　115
コホモロジー論　125

サ

三角不等式　8
3 次曲線　29, 33
自己準同型環　145
弱有限生成定理　70
終結式　95
種数　37
種数 0　3
種数 1　36, 39, 107
主等質空間　134
生成点　75
双有理同値　4

タ

大域体　16
退化した曲線の群構造　47
対称的　22
対数的高さ　103
楕円曲線　39
高さ　99
玉河数　142
単位元　33
超距離不等式　8
重複度　29, 53
同種写像　75
特異　29
凸　22

ナ

ニュートン　30
ノルム　85

ハ

判別式　97
非アルキメデス的付値　8
標準形　39
標準的高さ　104
付値　7
忘却関手　95

マ

持ち上がる　52

ヤ

ヤコビ多様体　121
有限位数の元　63

有限基底定理　*102*
有限生成定理　*69*
有理曲線　*3*
有理的　*3*

ラ

離散位相　*129*
例外的　*30*
レベル　*58*
連続なコサイクル　*129*

楕円曲線入門　J.W.S.キャッセルズ

1996年1月25日　第1刷発行
1997年4月7日　第3刷発行

訳　者　徳永浩雄（とくながひろお）

発行者　安江良介

発行所　株式会社　岩波書店
〒101-02 東京都千代田区一ツ橋 2-5-5
電　話　案内 03-5210-4000

印刷・法令印刷　カバー・半七印刷　製本・桂川製本

ISBN4-00-005642-5　Printed in Japan